Annual Information Risk Report 2018/19

Created by	Information Governance
Date	8/2/19
Reviewed by	Tariq Slaoui
Date	3/7/19

Document Control

Version	Date	Author	Notes / changes
V0.1	08/02/19	Mark Bleazard	Initial draft based on previous report
V0.2	09/04/19	Tariq Slaoui	Revised update
V0.3	22/05/19	Tariq Slaoui	Revised update
V0.4	06/06/19	Tariq Slaoui	Revised update
V0.5	11/06/19	Mark Bleazard	Updated
V0.6	14/06/19	Mark Bleazard	Updated
V0.7	18/06/19	Tariq Slaoui	Updated
V0.8	21/06/19	Mark Bleazard	Updated
V0.9	24/06/19	Tariq Slaoui	Updated
V1.0	01/07/19	Mark Bleazard	IGG consultation comments
V1.1	03/07/19	Mark Bleazard	Final review for Management Scrutiny Committee

Table of Contents

Contents

Executive Summary 1

1. Background and Purpose 3

1.1. Purpose of the Report and Benefits 3

2. Current Position 3

2.1. Compliance and Audit 3

Public Services Network (PSN) compliance 4

General Data Protection Regulation (GDPR) 4

Payment Card Industry Data Security Standards (PCI-DSS) 5

Cyber Essential Plus 6

Wales Audit Office (WAO) 6

2.2. Information Governance Culture and Organisation 6

Information Governance Culture 6

Organisation 6

2.3. Communications and Awareness Raising 8

Staff Guidance 8

Training Courses 8

Information Policy Development 10

2.4. Information Risk Register 10

2.5. Information Security Incidents 11

2.6. Information Sharing 12

2.7. Business Continuity 12

2.8. Technology Solutions 13

2.9. Records Management 15

2.10. Freedom of Information and Subject Access Requests 15

3. Risk Management and Associated Action Plan 17

3.1. Risk Management 17

3.2 Action Plan 20

Executive Summary

The council has a statutory requirement to look after the data it holds in line with General Data Protection Regulation (GDPR) and the associated Data Protection Act 2018. As a result of GDPR, the Information Commissioner's Office (ICO) has the power to fine organisations up to **20 Million Euros or 4% of turnover.**

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

- Compliance and audit
    - **Public Services Network (PSN) accreditation achieved in November 2018**
        - Annual IT Health Check and associated remediation action plan needs to be completed prior to PSN expiry in November 2019
    - **General Data Protection Regulation (GDPR). Progress was made in a number of areas**
        - Particular emphasis on the development of privacy notices across the organisation.
        - **A Data Protection Policy was developed to communicate the rights of individuals to staff,** especially around Subject Access Requests
        - Data Protection Impact Assessment (DPIA) carried out for Customer Relationship Management (CRM) system
    - Payment Card Industry (PCI) standard
        - Work required for PCI following previous audit

- Information Governance culture and organisation
    - Continue to develop and manage relationships with Shared Resource Service (SRS)
    - Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders including Shared Resource Service
    - Quarterly meetings of Data Protection Group to discuss operational data protection issues
    - **As a result of a change in guidance, Newport City Council councillors are no longer required to be registered individually as data controllers under the Data Protection Act**
    - **Action plan required to take forward agreed Service Level Agreement with primary schools**

- Communications and Awareness Raising
    - Continue to raise awareness with staff
    - **Members training took place with very good attendance**
    - Good level of attendance in Social Services and corporately
    - Update of a number of policies as a result of GDPR

- Information Risk Register
    - Continues to be maintained with contribution to Annual Governance Statement

- Security incidents
    - An increase in reported incidents, possibly as a result of increased awareness around issues as a result of GDPR
    - On-going management of incidents
    - Two incidents reported to the Information Commissioner's Office (ICO) during 17/18. Both were 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 all systems from tape to disk. The next phase is to provide access to key systems should both server rooms at the Civic Centre not be available.

- Technology Solutions
    - **Roll out of Office 365 for e-mail in cloud including Microsoft Multi Factor Authentication (MFA) and Advanced Threat Protection (ATP)**
    - Extend use of Xerox Mail solution to improve mail distribution processes

- Records Management
    - Continued roll out of EDMS solution across council
    - Review options for Modern Records and storage

- Freedom of Information
    - **Exceeded target for year**
    - **Highest number of request received since records began**
    - Publication of further open data sets and adding new ones where appropriate

- Subject Access Requests
    - Guidance to staff included in new Data Protection Policy
    - Need to ensure all Subject Access Requests are recorded in FOI system and processed in line with Data Protection Policy

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 now defined in EU General Data Protection Regulation (GDPR) and the associated UK Data Protection Act 2018 that places a greater responsibility on the council. The council must continue to meet its statutory responsibilities effectively and **protect the personal information it holds throughout its life cycle;** from creation through storage, use, retention, archiving and deletion. GDPR requires organisations to be more clear and transparent about what data is processed and how to give citizens confidence that their data is being handled appropriately. The principle of using and securing data is outlined in the Digital Strategy. Data is a valuable organisational asset and a key development is the creation of the Newport Intelligence Hub. This team's role is to maximise the value of data to the organisation, especially for use in operational, tactical and strategic decision making by the organisation. This requires processing of information in line with GDPR.

The actions outlined in this report form part of the People and Business Change service plan and are 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 seventh Annual Information Risk Report.
- Identify and address weaknesses and develop an action plan
- Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties. The fines associated with General Data Protection Regulation (GDPR) came in to place on 25th May 2018 with a maximum fine of 20 Million Euros or 4% of turnover. 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

As detailed in last year's report, an annual IT Health Check was undertaken by an approved contractor. As a result of some scheduling issues, this was later than planned. The original submission was rejected in May 2018 but following re-submission accreditation was achieved in November 2018. Consequently, PSN compliance is now valid until November 2019. To avoid scheduling issues, the annual IT Health Check is planned for July 2019 to give appropriate time to resolve any vulnerabilities identified. The Shared Resource Service (SRS) now procures and schedules health checks for partners together which simplifies and streamlines the process. The number and variety of risks mean that work is required throughout the year to protect the council's data and systems. Risks around cyber security remain a specific concern such that they are included on the Corporate Risk Register and this remains a challenge to all organisations whether public or private sector. The council is committed to continued compliance with PSN standards.

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the European Council and the European Commission strengthens and unifies data protection for individuals within the European Union (EU). GDPR came in to force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. As well as greater responsibilities on data controllers, the theme is to be more open and transparent to citizens in terms of how their data is processed.

There are major implications as a result of GDPR and this is a standard agenda item for the Information Governance Group. A GDPR Task and Finish Group has now changed in to a new Data Protection Group.

A summary of some of the changes are detailed below:

- The maximum fine is 20 Million Euros or 4% of turnover
- There is now a requirement to document the personal data held and keep a record of our processing activities.
- Data breach reporting is now mandatory for certain data breaches. The ICO should be informed of significant data breaches within 72 hours.
- Enhanced rights for data subjects. Privacy notices are now mandatory and the organisation must identify a 'lawful basis' for each of our processing activities. Consent has been strengthened. However, this is just one of a number of lawful bases. Specific guidance relating to children and their rights
- Local authorities can no longer rely upon "legitimate interests" as a legal basis for processing data
- The removal of maximum fee for Subject Access Requests and reduction in days to process (from 40 calendar days down to 30)
- Requirement for Data Protection Impact Assessments, particularly for new projects and/or technology implementations.
- Requirement for Data Protection Officer role
- Further consideration of data stored outside the EU

A GDPR Task and Finish Group was established in 2017, with representation from each service area and schools. With the assistance of the group, the council has progressed 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 across the organisation, to provide specialist input. An intranet presence has been set up and content uploaded. E-bulletins have been issued to provide corporate updates. Specifically, a communications campaign has been undertaken to ensure that staff are aware of the process to follow for Subject Access requests (SAR's).

- Communicating Privacy Information – under GDPR, the council will need to demonstrate proactively to individuals, how we are processing their data. A Corporate Privacy Notice has been developed and published to allow us to be more accountable and transparent about this. The task and finish group has undertaken a forms audit to understand what types of personal data we are collecting from individuals and to establish a lawful basis for processing this data. This forms audit has recently been revisited to identify any gaps and work is currently underway to ensure that all appropriate services are covered.
- Consent – the rules around consent have been significantly strengthened under GDPR. A consent checklist has been drawn up to assist mangers/service areas who rely on consent as the lawful basis for processing personal data. It is important to recognise that consent is only one of six lawful bases under GDPR and consent should only be used where the other lawful basis have been ruled out. The Information Management team continue to provide advice and guidance to service areas in this respect.
- Data Protection Impact Assessments – DPIA's are now mandatory for new technology implementations and projects that involve the systematic monitoring of individuals and/or the large scale processing of special category data. A DPIA was conducted for the Customer Relationship Management (CRM) implementation and the Civil Parking Enforcement systems will require a DPIA. Others are being considered but the screening process will ultimately determine this. The SRS have confirmed that all technology requests from Newport City Council are subject to DPIA screening.
- Incident Reporting – the Information Security Incident Reporting Policy is aligned with the requirements of GDPR and the key points have been communicated to the organisation. As noted above, the maximum fine is now 20 Million Euros or 4% of turnover and there is a specific requirement to notify the ICO of significant breaches within 72 hours. In certain circumstances, there will be a requirement to notify data subjects of breaches of their data. Staff have been advised to report any suspected incidents to the information management team in a timely manner.
- The Information We Hold – Tte accountability principle states that we should document the data that we hold along with records of processing activities. The council already manages an Information Asset Register which is based upon the systems that have been identified as a priority. The Data Protection Group is currently working to expand this register to other areas of the authority, and to include paper records.
- The rights of individuals – the rights of individuals and how to access them under GDPR have been reflected in the privacy notices published (see above). We have published our new Subject Access Request procedure, to align us with the requirements of GDPR. The discretionary £10 fee has been removed and we have formally reduced the amount of time that we have to process a request, from 40 calendar days, down to 1 month. The new process has been extensively communicated to the organisation.
- Data Processor/Joint Controller responsibilities – Data Processors (organisations who process personal data on our behalf/contractors) and joint controllers have further obligations under GDPR. Where possible, we have contacted those organisations and communicated the changes to them. The procurement team have now updated all new contracts to reflect the new GDPR clauses
- Staff Training – Information Security Training has been updated to cover all aspects of GDPR. The information management team have developed a GDPR e-learning module to facilitate desktop learning. This module is in the final stages of production and will be released very soon.
- Data Protection Policy – a Corporate Data Protection Policy was developed and agreed following all member consultation. This will now be published and communicated to the organisation.

Payment Card Industry Data Security Standards (PCI-DSS)

The council was previously compliant with Payment Security Industry (PCI) Data Security Standards. A previous audit identified issues to be addressed. An action plan has been developed by the SRS in conjunction with the Information Management team and the actions will be scheduled in 2019. Accordingly, the council's PCI compliance has lapsed to ensure these issues are formally resolved to meet PCI requirements.

Cyber Essential Plus

Welsh Government has provided funding for 2 years to facilitate local authority accreditation to Cyber Essentials Plus. The Cyber Essentials Plus project is a project by the Welsh Local Government Association (WGLA) to ensure that all 22 local authorities and the 3 fire & rescue services in Wales are certified to Cyber Essentials Plus (as well as IASME certification). Newport City Council has commenced work on this in conjunction with the SRS and a submission is planned in July 2019.

Wales Audit Office (WAO)

The Wales Audit Office (WAO) carries out audits annually which involve IT and Information Governance. Currently work is planned for this to take place in June 2019.

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. Since then, representatives from the SRS attend various Newport City Council groups. There is also a client side role sits within the Digital team and this relationship has developed since joining the partnership.

Information Governance Culture

The information governance culture has previously been investigated by virtue of staff surveys. These demonstrated good staff awareness of information governance issues and good buy in. A revised survey has been designed incorporating some previous and some new questions. At time of writing, this survey is being finalised, with analysis planned for an updated version of this report.

Organisation

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

Data Protection Officer Role

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

Shared Resource Service (SRS) - The IT Service became a partner in the Shared Resource Service (SRS) on 1/4/17. As well as Newport City Council the SRS is made up of Torfaen County Borough Council, Monmouthshire County Council, Blaenau Gwent County Borough Council and Gwent Police. There is SRS representation on the council's Information Governance Group as well as other groups such as the Digital City Board. The client side role is managed by the Digital team and this important relationship in service delivery as well as information governance continues to develop. The SRS has a complementary role of Information Security Architect who works with the Information Management team in Newport.

Councillor Data Protection
All councillors were registered as data controllers under the Data Protection Act in 2018/19. Following Information Commissioner's Office (ICO) guidance from 1 April 2019, *the Data Protection (Charges and Information) (Amendment) Regulations 2019 exempted the processing of personal data for:*

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

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

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

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

Information Asset Register - the development of an Information Asset Register, based on a template from The National Archives was completed for priority systems during 2016/17. This identifies the owner of information, the information stored within the system, how this is shared and various other pieces of information. This is being extended to meet the requirements of General Data Protection Regulation (GDPR) and is due to be completed during 2019.

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

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

Schools
Schools are "data controllers" under the Data Protection Act and therefore need to be equipped to handle data appropriately. Guidance is provided to schools by staff in Education and Information Management. At the time of writing, a proposed Service Level Agreement (SLA) for primary schools with the Information Management team appears to be going forward. This will provide a service to primary schools similar to that being provided corporately.

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 has been revised to reflect the new Data Protection Act 2018. The team regularly assess information from the Information Commissioner's Office (ICO) to ensure that key messages are communicated to employees including good and bad practice.

Training Courses

The council continues to provide classroom style training to staff to provide the most interaction possible and improved learning experience. This complements e-learning required to be completed by new starters. The content had minor updates to reflect events and keep it relevant. A major revision of the training content was undertaken to reflect GDPR (see further details within this report). The courses run are:

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

Training courses represent a continued commitment to information security by the council. Training is a key area as people are generally considered the weakest link in relation to information security. There will never be totally comprehensive technical measures to protect data. Training provided to staff is a key part of investigations carried out by the Information Commissioner's Office (ICO) as highlighted in the 'Security Incidents' section below.

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 was particular emphasis on Social Services training following a serious incident reported to the Information Commissioner's Office (ICO) in 2015/16. Training capacity was doubled in response and this incident was closed with no further action by the ICO and the gaps in training provided were filled. As such, generally one course per month was run during this year. Therefore, in 2018/19 the number of staff that attended was 157 which compares with 237 in 2017/18 where there was a specific training gap to fill.

A breakdown per year is included below.

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

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

Corporate Courses

These courses continue to be scheduled on a monthly basis, primarily for staff other than Social Services. The number of staff that attended the corporate course was 105 compared with 114 in 2017/18. Whilst attendance does vary a little year on year the number of staff attending remains consistent.

Year	Number of staff who attended
2018/19	**105**
2017/18	114
2016/17	118
2015/16	114
2014/15	152
2013/14	93
2012/13	57

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

Councillor Courses

Three sessions took place during November 2018 with 24 out of the 50 Councillors attending. Councillors, like all council staff, need to undertake mandatory e-learning before they are provided with access to the council’s network. As detailed elsewhere in this report, whilst all Councillors were registered as data controllers this is not now required following ICO guidance.

Schools Courses

No specific information security courses for schools were run during 2018/19.Schools have been engaged with in relation to GDPR including representation on the task and finish group. As above a proposal made for a service level agreement for primary schools for information management appears to be agreed and this would include regular training.

Other Courses and Presentations

Given specific operational requirements for the Registration Service, a training session was run for Registrars attended by a total of 21 staff. The information Management team also presented at the GEMS training day and visited the Information Station to deliver data protection training.

Information Management Team Training

All current members of the Information Management team have passed the British Computer Society (BCS) Certificate in Data Protection including two members of staff on the updated legislation.

E-Learning

All staff that need access to the council's computer network are currently required to undertake e-learning before they can access the network and this e-learning was revised during the year. This is being revised and new staff will be provided with information on their obligations under the Data Protection Act 2018. The e-learning is also published on the intranet as reference to staff and as a refresher.

Information Policy Development

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

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

Updated Policies

The Information Security Incident Reporting Policy has been reviewed and updated to reflect changes required for GDPR (see elsewhere in the report). Policies are also reviewed generally to ensure that they are still valid and up to date. The following policies have been updated:

- Access To Network and Email Policy
- Information Security Incident Reporting Policy
- Building Access Policy
- Physical Access Policy
- Disposal of IT Equipment/Mobile Phones
- Confidential Waste Policy
- Information Risk Management Policy
- Information Retention and Disposal Policy
- Records Management Policy
- Information Sharing Policy
- Document Services Physical Access Policy
- Protectively Marked Information Handling Policy

Staff are made aware of policy changes with reminders through the regular staff bulletin. All policies use 'key messages' for ease of understanding and are published as part of the overarching Information and IT Security Policy and on the Council's intranet, with appropriate version control.

2.4. Information Risk Register

An information risk register is maintained that identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. The risk register is regularly shared with the Information Governance Group to keep them informed of risks and is maintained by the Information Management team. Cyber Security remains a risk that needs to be managed.

Information risks are considered as part of the council's Annual Governance Statement and the Corporate Risk Register. The Chief Internal Auditor is a member of the Information Governance Group which helps to join up services. Cyber security is the only current information risk that is deemed significant enough to be incorporated on the Corporate Risk Register. 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.

46 security incidents were recorded in 2018/19 compared with 34 in the previous year. This is an increase from last year which was the lowest number of recorded incidents. 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.

Details of reported incidents over previous years are provided below:

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

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

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

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

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

The most significant incidents during this year were:

A Council Tax incident was reported to the ICO – a system configuration error in our hybrid mail system resulted in the incorrect combining of some Council Tax letters into the same envelope. As approximately 150 customers were affected it was agreed to report to the ICO. After consideration, the ICO took no formal action. This was based upon the small amount of personal data included in the letters, the speed in which we resolved the issue and the action already taken by the authority in response to the incident.

A Housing data incident was reported to the ICO - A former council employee retained notebooks belonging to the authority after their employment. The notebooks contained information relating to a range of matters, including personal information about employees as well as clients. Following our investigation, again the ICO took no formal action.and subsequently the notebooks were returned to the authority.

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 2018/19:

Information Sharing Protocols (ISP's)

An ISP for Newport's Not in Education, Employment or Training (NEET) Partnership is currently under development.

Data Disclosure Agreements (DDA's)

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

Data Disclosure Agreements have been developed as follows:

Finalised DDA's in 2018/19:

- Primary school to secondary school data transfer
- Live Birth Data
- Children in Need Census/SAIL (Secure Anonymised Information Linkage)

2.7. Business Continuity

There is an ever increasing reliance on digital technology to support business activities and it is therefore important to maximise the availability of systems. Increased resilience was a factor in the decision to join the Shared Resource Service (SRS). The SRS provides an on call service and the systems covered by the SRS in this arrangement are currently under discussion.

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 all systems from tape to disk. The next phase is to provide access to systems should both server rooms at the Civic Centre not be available. The SRS is leading on this with the Digital team to progress this work although this may change due to changing demands and IT system changes.

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 migrated its e-mail solution during the last half of this year to Microsoft Office 365. This means the use of Office 2016 and e-mail within the cloud. This provides improved collaborative, agile working facilities and information security. The solution uses Microsoft Multi Factor Authentication (MFA). In addition, the Microsoft Advanced Threat Protection (ATP) solution was implemented to protect against attachments and links sent in e-mails. The e-mail configuration includes the use of Transport Layer Security (TLS) to encrypt e-mail to external e-mail systems set up to the same standard which should include all local authorities and the public sector generally. In addition, some work has been carried out to implement Domain-based Message Authentication, Reporting & Conformance (DMARC).

Digital Champions
The council has approximately 30 “Digital Champions” who are advocates for the use of digital technology. They provide a key contact point for services using digital technology. They were a key part of the testing for Office 365 as above.

Mobility solution
The use of a mobility solution is 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. The solution now uses Microsoft Multi Factor Authentication (MFA) as used for Office 365 access.

Secure/Large File transfer solution
Egress Switch is rolled out to all users. This enables the secure transfer of e-mails and associated documents to organisations and individuals without secure e-mail facilities. The solution provides the ability to restrict access to specific documents and audit access to the information provided. It also allows large files to be safely shared via email. The solution is live with enhanced Data Loss Prevention (DLP) facilities to scan e-mail for personal data which prompts users to encrypt e-mail if they include certain pieces of sensitive data. In line with the implementation of Egress Switch generally, the council will remove personal network storage for staff wherever possible.

Xerox Mail “hybrid mail”
A new “hybrid mail” system is 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 will be rolled out to other parts of the organisation to maximise the benefits to the council. This solution provides financial savings and reduces information risk.

Desktop Technology
The council continues to increase the percentage of laptops as part of its total number of computers used to encourage more flexible and agile working with access to information and records from a variety of locations. Laptops now represent approximately 70% 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 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 in October 2017 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. A small number of suppliers who may be required to support IT systems outside IT hours have a new solution using Microsoft Multi Factor Authentication (MFA).

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

Wireless Staff Access
Wireless Access points are provided in many council buildings. This includes appropriate security controls in place. Various updates have taken place in 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), over 50 public buildings and on public transport (Newport Community Cloud). Friendly Wi-Fi accreditation has been achieved for this set up. Gov Wi-Fi is available in various public buildings too.

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

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

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

Digital and Technology Developments
The council's Digital Strategy outlines strategic objectives including a move to more 'cloud' based technologies. 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

The implementation of the corporate Electronic Document Management System (EDMS) across services includes retention facilities that assists with GDPR An upgrade to the Social Services system took place and a similar upgrade to the corporate system is planned. EDMS provides the council with a modern, efficient, electronic system for managing documents, improving the way information and documents are used and the flow of information around the council. Documents are scanned on receipt into the mail room, and made available to services in the EDMS system.

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

2.9. Freedom of Information and Subject Access Requests

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

Freedom of Information
This is the fifth time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2018/19 was 1,167 which is an increase from last year of 130 requests or 12.5%. 2016/17 was the first time that the number of requests had reduced from the previous year. since records began in 2011/12. Following the reduction in 2016/17 the figure for 2017/18 represents the highest number of requests ever recorded. It is 80 more requests received than the previous highest number. It is always difficult to understand the reasons behind variation in numbers as there are a number of factors that may impact on the figures, especially issues that are of particular local or national interest e.g. Brexit. These tend to generate a number of FOI requests and the number tends to reflect the level of public interest. Performance for 2017/18 was 90.0% of requests responded to within 20 working days. This was above the target of 88% of requests. The council has met its target for six of the eight years since a target was identified.
.
A breakdown per year is included below:

Year	Number of requests	Performance (Target)
2018/19	1167	90.0% (88%)
2017/18	1037	88.3% (88%)
2016/17	1087	84.1% (88%)
2015/16	914	92.3% (87%)
2014/15	895	87.7% (87%)
2013/14	869	87.1% (87%)
2012/13	698	90.4% (87%)
2011/12	540	84.4% (87%)

The existing system for managing FOI requests has been extended further with options being considered for future years including use of the new CRM system.

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

This page includes:

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

Housing information and Contact Centre statistics were added this year. 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. As a result of General Data Protection Regulation, fees have not been charged since April 2018 prior to the May deadline. As detailed above, a new Data Protection Policy was developed and this includes the rights of individuals under the Data Protection Act 2018. Specific guidance on processing Subject Access Requests is included in the policy and guidance to staff has been provided on the intranet and in staff bulletins. The personal information request form used to identify specific subject areas for requests as well as gathering details of the requestor was amended to reflect the removal of any fee. It is crucial to gather proof of identity so personal data is not disclosed to a third part accidentally.

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 is a very large task.

GDPR means that organisations need to be clearer and more transparent about how they process data. Many of the processes and tasks required to comply with this are well advanced with excellent progress made. In addition, organisations need to get a better understanding of what data they hold and the legal basis for the processing and this is well progressed with some work to do. Citizens are also provided with enhanced rights and these are detailed in a new Data Protection Policy which provides guidance to staff and special emphasis on processes for Subject Access Requests. Information risks change regularly and these are managed by the Information Management team by an information risk register and other processes Evidence to date suggests that the ICO will not issue organisations, especially the public sector, with excessive fines. The theoretical maximum fine is now 20 Million 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.

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

The Information Governance Group continues its important work of monitoring risk across services and providing strategic direction with representation form the Shared Resource Service (SRS) and this will require a different method of operation. The SRS client side role continues to develop and this is recognised as a crucial area to meet the digital needs of the council as an SRS partner organisation. The aim is for improvements in information security across all partners by a simplified and standardised infrastructure where possible and 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 data protection 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	Undertake IT Health Check and resolve any vulnerabilities identified. Evidence information governance arrangements as detailed in this document. Ongoing patch management and	Digital Services Manager (DSM) in conjunction with in conjunction with SRS

			other activities to reduce risks. Continued engagement with Members	
Delivery of IT Service by Shared Resource Service (SRS) provides less control	M	M	Continue to develop relationship with the SRS Develop client side role to provide strategic input and performance monitoring	Digital Services Manager (DSM) in conjunction with Head of PBC / SRS management
Do not meet requirements of EU General Data Protection Regulation	M	M	Staff Awareness raising especially senior management GDPR tracker being managed and shared with Data Protection Group Standing agenda item at Information Governance Group	Digital Services Manager (DSM) in conjunction with Head of PBC / SRS management
PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	Complete actions identified in audit report	Digital Services Manager (DSM) in conjunction with in conjunction with SRS
Technical Solutions are not available to meet the needs of service delivery and data breach occurs	H	L	Microsoft Multi factor Authentication (MFA) solution for secure access to office 365 e-mail. Egress Data Loss Prevention (DLP) system rolled out and other improvements to e-mail security Encrypted laptop devices New Multi-Function Devices (printer/copier) has increased security features Data stored on servers and not on local devices unless encrypted Review solutions, identify and plug any gaps Maintain health check and compliance requirements Review the security of cloud based technical solutions considered	Digital Services Manager (DSM) in conjunction with Information Management team
Information is not shared appropriately and securely	H	L	Development of new Information Sharing Protocols and Data Disclosure Agreements and review of existing ones Advice and guidance	Digital Services Manager (DSM) in conjunction with Information Management team
Critical IT systems are not available to services	H	L	Phase 1 of disaster recovery solution completed by SRS. SRS now progressing to phase 2 to provide alternative processing facilities. Continue to review and refine priorities for critical IT	SRS in conjunction with Digital Services Manager and services

			systems and ensure these are communicated to relevant staff. Work with SRS to develop consistent IT system priorities across partners where possible	
Information security is not considered for new projects	M	L	Data Protection Impact Assessments (DPIA's) carried out for new projects with further DPIA's required going forward. Use ICO process including screening	Digital Services Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Carry out annual IT Health Check and associated remediation action plan prior to PSN submission	Oct 19
EU General Data Protection Regulation (GDPR) and DPA 2018	
GDPR to be discussed as standard item at Information Governance Group and Data Protection Group	On-going
Finalise forms audit and associated privacy notices for the organisation. This will include the legal basis and consent where appropriate	Aug 19
Information Asset Register to be reviewed, updated and extended as necessary	Sep 19
Privacy notice and DPIA for Civil Parking Enforcements systems	Jun 19
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
PCI accreditation	
Payment Card Industry Data Security Standard actions as a result of audit to follow prioritised PSN work	Aug 19
Cyber Essentials Plus	
Submission for Cyber Essentials Plus	Jul 19
Information Governance Culture and Organisation	
Circulate and analyse data protection staff survey	Aug 19
Continue to develop and manage relationships with Shared Resource Service (SRS)	On-going
Contribute to information governance considerations across all SRS partners	On-going
Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders including Shared Resource Services representation	On-going
Quarterly meetings of Data Protection Group to discuss operational data protection issues	On-going
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Members updated through Annual Information Risk Report, including review by Scrutiny Committee	Jul 19
Develop action plan to take forward agreed Service Level Agreement with schools	Jul 19
Communications and Awareness Raising	
Regular data protection training sessions corporately and for Social Services including additional monthly courses to meet demand	On-going
Further policies and guidance will be developed to support the organisation	On-going
Information and IT Security policy to be reviewed in reference to Data Protection Policy	Sep 19
Existing policies and guidance will be reviewed and updated to ensure they are appropriate	On-going
Provide advice and guidance to support primary schools in conjunction with planned Service Level Agreement	On-going
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 to enable key systems to be accessed should both server rooms at the Civic Centre not be available.	Mar 20
Work with Shared Resource Service to agree and communicate out of hours on call systems	Sep 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
Ensure information security is appropriate around Office 365 solution including Multi Factor Authentication	Apr 19
Extend use of Xerox Mail solution to improve mail distribution processes	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
Records Management	
Continued roll out of EDMS solution across council	On-going
Review options for Modern Records and storage	On-going
Freedom of Information and Subject Access Requests	
Freedom Of Information	
Publication of further open data for suitable data sets	On-going
FOI system options being considered including use of the new CRM system	Dec 19
Subject Access Requests	
Ensure all Subject Access Requests are recorded in FOI system and processed in line with Data Protection Policy	Apr 19