Public Document Pack

Agenda

Cabinet Member for Community Services, Work & Skills

Date: Friday, 12 August 2016

Time: Not required

Venue: Not required

To: Councillor R Jeavons

Item		Wards Affected
1	Annual Information Risk Report 2015-16 *(Pages 3 - 36)*	

Contact: Anne Jenkins, Democratic Services Officer
Tel: 01633 656656
E-mail: anne.jenkins@newport.gov.uk
Date of Issue: 4 August 2016

This page is intentionally left blank

Report

Cabinet Member for Community, Work and Skills

Part 1

Date: 12 August 2016

Item No: 1

Subject **Annual Information Risk Report 2015-16**

Purpose To provide an assessment of the Council's information governance arrangements, identify key risks and agree the action plan for 16/17.

Author Information Development Manager, Digital and Information Manager

Ward General

Summary Local Authorities collect, store, process, share and dispose of a vast amount of information. The Council must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation through storage; use, retention, archiving and deletion.

The purpose of the council's fourth Annual Information Risk Report is to provide an assessment of the information governance arrangements for the Council and identify where further action is required to address weaknesses and make improvements.

Proposal **To endorse the Annual Information Risk Report 2015-16 and proposed actions.**

Action by Information Development Manager Head of People and Business Change

Timetable As reported

This report was prepared after consultation with:

- Head of Law and Regulation – Monitoring Officer, and Senior Information Risk Owner (SIRO)
- Head of Finance – Chief Financial Officer
- Head of People and Business Change
- Chief Internal Auditor
- Information Governance Group
- Scrutiny Committee Planning and Development

Signed

Background

The purpose of this report is to provide an assessment of the information governance arrangements for the council and identify where action is required to address weaknesses and make improvements. The benefits of the report are as follows:-

- Provide an overview of the council's information governance arrangements;
- Highlight the importance of information governance to the organisation and the risks faced;
- Enable comparison of performance over time;
- Identify and address weaknesses and develop an annual action plan;
- Reduce the risk of failing to protect personal data and suffering any subsequent reputational and financial penalties (the Information Commissioners Office can issue a fine of up to £500,000 for data breaches).

Scrutiny

The draft report was considered by the Scrutiny Committee for Community Planning and Development in June 2016 who endorsed the report and proposed action plan.

The questions and comments of the Scrutiny Committee were as follows:

- Members questioned who was the responsible Officer in the Authority and whether there was political responsibility for breaches? – It was confirmed that the Senior Information Risk Owner (SIRO) is the responsible Officer in public sector organisations and that in addition to potential fines from the ICO as a result of a breach, there is also reputational damage for Officers and Members if public information is lost. The process and arrangements put in place minimise the risk but it cannot be eradicated altogether.
- Has the reduction of the number of staff over the past 4 to 5 years increased the risk? – Whilst organisationally every necessary step can be taken, with 5,500 staff the biggest risk is paper records not electronic as electronic devices are encrypted. There are less staff and they are working hard, so risk could increase, but there are policies to control paper and there is external scrutiny of Information Management from Wales Audit Office, ICO etc. It was also explained that the number of organisations the Council interacts with, e.g. Health, Police, Voluntary sector, etc. and the way we work including agile working result in new risks, and this is mitigated by policies, procedures and sharing protocols.
- Concern was expressed that the pressure to reduce costs can create problems but systems are in place to prevent otherwise if there is too much pressure then there is an increased risk.
- Of the 62 security incidents in 2015/16, 2 related to lost or stolen paperwork but 23 related to disclosed in error. Those disclosed in error relate to paper and electronic records and the risk is being managed.
- Is there a risk from papers left on photocopiers? – Recently updated systems to address this and should improve. Anyone finding on the printer should be an internal member of staff and should destroy it. Printers have to be swiped with id cards to log on, before printing can commence.
- While it would be good to have fewer incidents, it is good that the 23 incidents are listed, have been investigated and the figures are reported openly and transparently.
- Is there more training now than 3 years ago? - 3 years ago there was a large push for training in social services, the percentage would be broadly similar, with targeted areas within the organisation and refresh 2 yearly. Although the figures for 5 years ago are not to hand, there is definitely more training being delivered now, as initially there was concentration on technical solutions such as locking down the software and firewalls.

- Have lessons had been learned from the security incident that was reported to the ICO this year and processes changed as a result? – There has been more training delivered and more guidance provided upon what is reasonable to have at home and to keep paper separate from IT kit and laptop bags.
- How is incorrect sharing of documents identified? How can we guarantee information is not being shared incorrectly? – All organisations are liable for the Data Protection Act and we build working relationships and trust with partners in terms of sharing information and through Information Sharing Protocols. The Council also shares information with non-statutory partners. e.g. domiciliary care providers and sets out the responsibilities for sharing information. Trust and professionalism encourages a culture of communicating any security incidents straight away.
- Would the partners be taken to task by ICO if incorrectly shared information? – Currently if it was our data the Council would be liable, but there would be reputational damage to the provider and trust issues. EU regulations are coming which share the responsibility for data with Providers. Any incident is investigated to identify data owner and processes and training to mitigate.
- It was clarified that subject access requests can be made by staff or members of the public to view the information the Council holds relating to them. Third Party information held on file cannot be shared without the party's consent being given first.
- Members of the Committee should attend a Member training session upon Data Protection. Details of the date of the course will be circulated once available.
- Have there been any new risks for information? – Particular viruses hitting national organisations. The paper risk remains the same but cyber risks are a challenge. Malicious attacks on IT systems are always going to be a risk. As the use of and reliance upon technology increases, the aim is to take the culture of the organisation along with it and be compliant. This may escalate over the next few years as staff numbers decrease and malware increases.
- The report also included Wales Audit Office recommendations around disaster recovery and a number of steps are being taken to improve this.

Monitoring progress

Progress on the action plan will be monitored by the Information Governance Group and as part of the People and Business Change service plan monitoring 16/17.

Financial Summary

There is no specific cost associated with the report. Any costs incurred would be normal costs associated with the running of the service. However, the report is designed to highlight risks and to reduce potential penalties from the Information Commissioner's Office (ICO) if information risk is not managed effectively.

Risks

A huge amount of information is held by the organisation. This needs to be managed appropriately. Further details of risks are provided in the report and those identified below represent some high level risks.

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Data breach results in fine imposed by the Information Commissioner's Office or reputational damage	H	L	All the actions detailed in this report are designed to mitigate this risk.	Digital and Information Manager and Information team

Council is unable to make best use of, and share the data it holds due to a lack of confidence in the integrity and security of the information.	L	H	Digital strategy sets the overall direction for the management of information. Day to day operational guidance provided by Digital and Information service.	Digital and Information Manager and Information team

* Taking account of proposed mitigation measures

Information Risk is also incorporated into Corporate Risk Register reporting, as outlined in this report.

Links to Council Policies and Priorities
The Council's Information Risk Management Policy sets out the Council's approach to information risk management including roles and responsibilities. The policy also details the processes in place to manage information risks effectively, including the Annual Information Risk Report.

The Digital Strategy, approved by Cabinet October 2015 sets the overall direction for the management of information, and information governance is also considered in the Annual Governance Statement produced for the inclusion in the Council's Annual Statement of Accounts and reported to Audit Committee. The actions outlined in this report form part of the People and Business Change service improvement plan from 16/17.

Options Available

1. **Do nothing**
2. **Note the annual information risk report and endorse its findings.**

Preferred Option and Why

The preferred option is option 2 – note the Annual Information Risk Report 2015/16 and endorse its findings. This will provide an understanding of the current position in relation to information governance and give an opportunity to monitor progress on actions identified

Comments of Chief Financial Officer

There are no direct financial implications within this report and the strength of the controls should minimise the potential of any significant financial fines from the Information Commissioner.

Comments of Monitoring Officer

There are no specific legal issues arising from the Report. The Annual Information Risk Report confirms that the Council has in place robust information governance arrangements and security policies to meet its statutory obligations under the Data Protection Act, FOIA, PSN accreditation and information sharing protocols. There has only been one significant security breach within the last 12 months involving a reference to the ICO and an action plan has already been put in place to address the issues identified and to avoid any recurrence of these problems.

Staffing Implications: Comments of Head of People and Business Change

There are no staffing implications associated with this report.

Risks regarding Information Management are included within the service planning process. The Annual Information Risk Report includes details of the management of the Information Risk Register and significantly high risks will be escalated accordingly.

Comments of Cabinet Member

There should be text clearly visible which should be added to all agendas to state “NB. Would members and officers please take any paper copies of the agenda with them after the meeting and please not leave unattended.”

Consultation

Comments of the Chief Internal Auditor

Having sound information governance arrangements in place strengthens the overall corporate governance arrangements for the Council. This report clearly demonstrates the Council has appropriate and effective arrangements in place for information governance and deals with further improvements in a transparent and inclusive way in order to minimise the likelihood of significant financial fines.

Background Papers

Information Risk Management Policy (reviewed November 2015).
Annual Information Risk Report 14/15
Annual Governance Statement 15/16
Corporate Risk Management Strategy and Register
Digital Strategy 2015-2020

Dated: 12 August 2016

Annual Information Risk Report 2015/16

Created by	Information Governance
Date	08/03/2016
Reviewed by	
Date	

Document Control

Version	Date	Author	Notes / changes
V0.1	08/03/16	Mark Bleazard	Initial draft based on previous report
V0.2	04/04/2016	Mark Bleazard	Updated draft
V0.3	25/04/2106	Mark Bleazard	Updated draft for Information Governance Group
V0.4	03/05/2016	Mark Bleazard	Further updates following Information Governance Group meeting
V0.5	17/05/2016	Tracy McKim	Further updates

Table of Contents

Contents

Executive Summary

The council has a statutory requirement to look after the data it holds. **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.**

This is the fourth 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 received. A number of vulnerabilities to resolve which is more challenging than last year
  - EU General Data Protection Regulation implications
  - Payment Card Industry (PCI) data security standards continued compliance achieved
  - Wales Audit Office – progress on recommendations including disaster recovery and business continuity

- Information Governance culture and organisation
  - Positive feedback from staff survey and evidence of improvement
  - Actions as a result of staff survey
  - Proposed joining of Shared Resource Service (SRS) for IT services represents a change that needs to be managed effectively
  - Training carried out for Information Asset Owners and agreement of Information Asset Owners and work on Information Asset Register to follow

- Communications and Awareness Raising
  - Continue to raise awareness with staff and members
  - Large amount of training provided to staff
  - Second programme of training delivered to Schools
  - Training for Members scheduled
  - Review of policies carried out including Schools IT Security Policy
  - Review of e-learning ongoing

- Information Risk Register
  - Continues to be maintained

- Security incidents
  - On-going management of incidents
  - One serious incident reported to the Information Commissioner's Office (ICO) pending response from ICO

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

- Business Continuity
  - Work resulting from Wales Audit Office (WAO) recommendation to test and improve disaster recovery and business continuity arrangements

- Technology Solutions
  - Complete roll out of Egress secure e-mail solution
  - Roll out of Xerox Mail solution to improve mail distribution and reduce errors from manual paper handling
  - Bring Your Own Device (BYOD) solution tested with roll out planned
  - Consider options and controls required for cloud

- Records Management
  - Continued roll out of Electronic Document Management Solutions (EDMS) solution across council
  - Good progress in improving management of paper records through ‘Modern Records’ facility

- Freedom of Information
  - Continue to meet targets despite increased request numbers
  - Publication of open data sets where appropriate

- Subject Access Requests
  - Improved processes developed with further roll out required

- New Projects
  - Public wifi across the city

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. The council must meet its statutory responsibilities effectively and **protect the personal information it holds throughout its life cycle;** from creation through storage, use, retention, archiving and deletion. The principle of using and securing data is outlined in the Digital Strategy.
The actions outlined in this report form part of the People and Business Change service plan and further detail incorporated in the Digital and Information 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 Council's Information Risk Management Policy sets out our approach to information risk management and roles and responsibilities. The policy is reviewed regularly and details the processes in place to manage information risks effectively, including the Annual Information Risk Report.

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 and the risks faced;
- Where relevant this report will compare performance with previous years and with the aim of continuous improvement;
- Identify and address weaknesses and develop an action plan;
- Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties (the Information Commissioners Office (ICO) can issue a fine of up to £500,000 for data breaches). 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.

This is the fourth Annual Information Risk Report and covers the period Apr 15-Mar 16.

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) which replaces the GCSx (Government Connect Secure Extranet) accreditation previously held. The council is also required to comply with the PCI-DSS Payment Card Industry Data Security Standards 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 (formerly GCSx)

Successful accreditation for PSN was received on 5th May 2016. Therefore the council's PSN compliance now expires on 5th May 2017. The successful accreditation will be followed up by checks of the council's remediation action plan to ensure continued compliance.

As noted in last year's report the Cabinet Office has a different approach which provides more flexibility for organisations enabling them to consider their own approach to risks. This does not actually change the fundamental requirements but places more responsibility on individual organisations. The risk of non-compliance within the required period would result in the Council being denied access to key systems such as the Customer Information System CIS from the Department for Work and Pensions (DWP) which is used by Housing Benefits.

EU General Data Protection Regulation

The review by the European Commission of European Data Protection legislation has resulted in an agreed EU Directive with implementation in member states in 2018. One of the main differences is that businesses will be subject to fines up to 4% of annual turnover which is a major increase in possible fines. In addition, mandatory notification of data protection breaches will be required by member states to their data protection authority (the ICO in the UK). The implications of this legislation need to be considered over the next year.

Payment Card Industry Data Security Standards (PCI-DSS)

The council made its first Self-Assessment Questionnaire (SAQ) for Payments Card Industry (PCI) data security standards in December 2014. Following this successful submission, the council has remained compliant. During this year, a new SAQ was completed with additional technical measures. Consequently the council is now successfully accredited to Version 3 of the PCI data security standards which expires on 22nd Feb 2017. 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.

As an extra safeguard, the council, in conjunction with its internal audit team, has commissioned an external audit of its PCI compliance to identify how well it adheres to the standards and any areas requiring improvement. The report on this exercise is expected shortly with appropriate actions to follow.

Wales Audit Office (WAO)

The Wales Audit Office (WAO) carries out audits annually which involve IT and Information Governance. In 2014 WAO completed a review of Information Governance and the outcome of this review and its recommendation are tracked by the Wales Audit Office as part of its monitoring of the council's corporate assessment.

As a result of WAO's recommendations the following actions have taken place.

- *Reminders to staff on reporting of information security breaches, supported by more streamlined processes.*
- *Change to role of SIRO to the Head of Law & Regulation, which is also reflected in the Information Risk Management Policy.*
- *Change to the chair of the Information Governance Group to Strategic Director (Place.*
- *Further information and training for staff.*
- *A test of disaster recovery arrangements with proposals for further improvements.*
- *Developing an understanding of information asset ownership and plans for an information register (ongoing).*

More detail on these actions is included in the relevant sections of this report. Wales Audit Office have reviewed progress as part of the 2016 work programme, this included the 2015 annual risk report and work of the Information Governance Group. The results of this review have not yet been received and will be included in later versions of this report if received.

The actions highlighted above show good progress against the WAO recommendations. The biggest challenges remain around Business Continuity/Disaster Recovery but significant progress has been made in this area.

2.2. Information Governance Culture and Organisation

The council's information governance arrangements continue to mature following the long term requirements of the Government Secure Extranet (GCSx) and its successor. The Information Governance Group was first set up in November 2013 and has continued to meet quarterly since. In addition, work has commenced on the identification of Information Asset Owners for implementation in 2016.

Information Governance Culture

In an effort to identify staff perception of the council's information governance culture, a questionnaire was provided on the council's intranet. The previous survey in 2013/14 was based on one developed by the CPNI (Centre for the Protection of National Infrastructure) and this year's results have been compared with the previous questionnaire results. The survey will be repeated in future to compare performance and identify areas to be addressed.

136 staff responded to the survey (114 in 2013/14) which again provides a good basis for analysis. As with other surveys of this kind, the answers to individual questions are important but the literal responses complement this by enabling staff to mention their own views and experiences.

77.9% of those who responded have been on information security training which suggests that most of the responses have come from relatively well-informed staff. This demonstrates good training take up but needs to be borne in mind when reviewing responses provided. A summary of the survey responses is below.

A number of yes/no questions were asked to get a view on items of specific importance. These are detailed below. Percentages shaded in grey relate to the 2013/14 survey for comparison.

Question	Yes	No	N/A	Comment
Do you know about the Council's training course?	**90.4%**	**9.6%**	**0.0%**	Awareness of the councils training course has improved significantly since the 2013/14 survey. Course details are published on the Council's Intranet and promoted in staff news bulletins.
2013/14 comparison	69.6%	30.4%	0.0%	
Have you been on the Council's course?	**77.9%**	**22.1%**	**0.0%**	77.9% of those who responded have been on the course which suggests that most of the responses have come from relatively well-informed staff. Training attendance is covered in section 2.3 of this report, training feedback responses are attached at Appendix A & B.
2013/14 comparison	53.2%	46.8%	0.0%	
Do you feel you have received enough training on information security?	**80.7%**	**18.5%**	**0.7%**	Although most feel the training received is sufficient, 18.5% feel that it was not enough. A training review took place in 2015 to ensure that the content remained relevant and up to date. E-learning to be reviewed and re-published.
2013/14 comparison	67.9%	31.3%	0.9%	
Do you know the correct procedure to follow in the event of an incident?	**74.1%**	**24.4%**	**1.5%**	24.4% do not know the correct procedure to report a security incident. This is an improvement since 2013/14, likely due to a policy review (Incident Reporting policy reviewed in 2014). Further communications to be arranged.
	64.3%	35.7%	0.0%	

2013/14 comparison					
Do you feel that you understand your own part in relation to information security?	92.5%	7.5%	0.0%	This is a new question introduced for the 2015/6 survey. The result suggests that employees are aware of their obligations, demonstrating that information security is recognised as important.	
Question	☺ **Strongly or somewhat agree**	😐 **Unsure or not applicable**	☹ **Strongly or somewhat Disagree**	**Aim**	**Comment**
Levels of information security are consistently high	68.4%	16.9%	14.7%	☺	Staff perceptions that levels of security are consistently high have improved since the previous survey. Staff comments suggest that a lot can be improved, particularly with paper based information.
2013/14 comparison	**61.4%**	**18.4%**	**20.2%**		
Access to sites, buildings, information etc. is effectively controlled	76.5%	8.3%	15.2%	☺	Although ¾ of staff agree with this statement, the comments suggest that there are still concerns about tailgating. Some comments suggest that staff are not confident enough to challenge this.
2013/14 comparison	**75.2%**	**9.7%**	**15.0%**		
Information security measures prevent me from doing my job effectively	19.6%	7.5%	72.9%	☹	This survey represents a 15.4% response improvement on the previous survey. 72.9% of staff currently disagree with this statement, however, comments suggest that IT/technology problems prevent staff from doing their jobs effectively. Lack of training on the use of Egress (secure email) was also widely commented upon.
2013/14 comparison	**18.6%**	**23.9%**	**57.5%**		
Sometimes I have to ignore information security measures in order to my job effectively	15.2%	6.8%	78.1%	☹	Most disagree with the statement which is positive. However, comments suggest that non-secure e-mail is being used to transmit confidential data. The Egress solution will improve this.
2013/14 comparison	**15.8%**	**14.9%**	**69.3%**		
Good information security practices and issues are regularly communicated to me	67.7%	11.3%	21%	☺	This suggests that awareness is improving with nearly 70% of staff agreeing. Some of the staff comments are asking for a greater variety of communication methods. Also suggests that we currently only communicate when things have gone wrong. We need to ensure that we communicate what we do well.
2013/14 comparison	**59.6%**	**20.2%**	**20.2%**		
My manager listens to my concerns about information security	74.6%	17.9%	7.4%	☺	A further improvement upon the 2013/14 survey. Senior managers have been encouraged to attend the information security training to support their staff. None of the comments suggest that managers do not listen to staff concerns.
2013/14 comparison	**64.0%**	**28.9%**	**4.4%**		

Staff Survey Literal Responses 2015/16

Q7: Do you agree or disagree that levels of information security are consistently high? – 32 comments received.
In general, the comments suggest that levels of information security are improving, especially with EDMS and Egress. Staff are happy with NCC's security, but less happy when transacting with other organisations. Staff take information security seriously, however, some concerns still exist;

Paper based information
Paper seems to be a particular area of concern with concerns over paper work taken outside of the Civic Centre. There are instances of letters being sent to the wrong customers. Paperwork has been found on printers, especially at the Information Station. Employees leave scraps of paper with confidential details in and around their workstations. The confidential waste procedure is not always being followed (to be reviewed 16/17)

Email
Computer workstations are sometimes left unlocked. Sensitive e-mails have been received in error. Schools have not been provided with Egress to date and there remains some confusion around which secure email solution to use;.

Q8: Do you agree or disagree that access to sites, buildings, information etc. is effectively controlled? – 26 comments received.
Comments are generally positive, physical security at Council buildings is very good. However, human error can lead to unauthorised access;

Tailgating
The comments focus largely upon the physical security of the Civic Centre. A number of staff raised concerns about visitor tailgating and unauthorised access to the building. Some comments suggest that unauthorised access through to staff only areas has been witnessed and that visitors have been found in stairwells etc. Staff need to be more confident in challenging people who do not wear an identity badge.

Q9: Do you agree or disagree that information security measures prevent me from doing my job effectively? – 21 comments received.
Technology breakdown can often lead to unwanted delay, however, when the technology is working, there is no evidence in this survey to suggest that information security measures prevent staff from carrying out their jobs effectively. The ability to self-release blocked email was seen as an improvement. The Egress solution was widely commented upon.

Egress
Some comments were complimentary. However, a number mentioned the lack of training/information and the delayed roll out to schools as causing confusion and lack of confidence in the system. Staff are asking for appropriate training. Communications on this implementation are ongoing.

Q10: Do you agree or disagree that sometimes I have to ignore information security measures in order to do my job effectively? – 10 comments received.
A mixed response with about 50% stating that they would never ignore security measures to carry out duties. Other responses state that if a secure email account holder is absent, they would send a confidential email via unsecure email, or that they have received confidential information from an unsecure email account.

Q11: Do you agree or disagree that good information security practices and issues are regularly communicated to me? – 7 comments received.
Responses are varied to this question. Some staff feel that the bulletin is not ideal for those who do not have access to computers. Others feel that more communication is required as it tends to

come in phases. More “good news” is required as it is perceived that we only communicate when there has been an error, mistake or breach.

Q12: Do you agree or disagree that my manager listens to my concerns about information security? – 10 comments received.
There were no reports of line managers not listening to the concerns of their staff. The comments suggest that managers act upon security concerns or refer to the information management team for advice, guidance or reporting procedures.

Organisation

Due to a change in the council’s structure, the council has changed the post of its named Senior Information Risk Owner (SIRO) role responsible for information security within the organisation. The role is now part of the Head of Law and Regulation post. Day to day operational management is provided by the Information Governance team that reports to the Head of People and Business Change.

The council agreed that its current preferred option for the delivery of its IT Service is to become a partner in the Shared Resource Service (SRS) which is currently made up from staff from Torfaen County Borough Council, Monmouthshire County Council, Blaenau Gwent County Borough Council and Gwent Police. If this development takes place as planned it will mark a significant organisational change in the delivery of IT services with a potential impact on information governance arrangements for the council. It is critical that relationships are maintained to deliver effective council services and part of this is the essential relationship with the Information Governance team.

An important aim of this report continues to ensure that members and senior officers are aware of the information security responsibilities of the council and to enable guidance to be provided. 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 proved a very useful process for all parties.

The Information Governance Group has met quarterly since its inception in November 2013. Following a recommendation by Wales Audit Office, the chair of the Information Governance Group is now the Strategic Director – Place. This was to ensure there was no possibility of a 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 being compliance update, information security incidents, training and awareness raising, risk report monitoring and other information governance updates. Membership of the group has been reviewed to provide improved coverage across the council’s areas.

As detailed in last year’s report, an important improvement is the nomination and development of Information Asset Owners (IAO’s). Training for Information Asset Owners was conducted by The National Archives. During 2016 this will be followed up by nomination of Information Asset Coordinators to complement Information Asset Owners. A formal information asset register for the council will also be developed for the first time. This demonstrates increasing maturity of information governance arrangements.

As noted last year, schools are their own “data controllers” under the Data Protection Act and therefore need to be equipped to handle data appropriately. To support schools, guidance is provided by staff in Education and Information Governance and a revised information security policy was developed. As detailed in the training section, four specific training sessions for schools were provided. As a consequence of these activities, there is increased awareness of information governance in schools.

2.3. Communications and Awareness Raising

Employees play a key role in information governance as demonstrated by the importance placed on training when incidents are reported to the ICO. As well as undertaking training it is important for staff to understand legal requirements and best practice and this can be driven by awareness-raising including staff bulletin articles, leaflets etc..

Staff Guidance

Regular reminders of good practice have been provided in the weekly staff bulletin and intranet and these continue to be regular and varied. Most notable is the communication to staff to minimise the amount of paperwork taken home and generally keep paperwork as secure as possible. This is as a result of the information security incident reported to the ICO.

The content of this advice continues to be recorded by the Information Governance team to evidence the messages communicated to employees. The information security leaflet provided to all staff that attend training has been amended 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 especially in the case of fines issued by the ICO to other organisations.

Training Courses

The council is committed to providing formal training to staff and a number of different courses are run. Social Services and corporate training courses have been reviewed and consolidated in to one standard course taking the best content from the previous two courses. The content has also been updated to make it as relevant and up to date as possible. The courses run are:-

- Social Services courses
- Corporate courses
- Councillor courses
- Schools courses
- Ad hoc courses and presentations
- Use of Electronic Document Management

These training courses are a significant part of the council's continued commitment to information security. Training is an important consideration when analysing security incidents and is a major consideration if incidents are reported to the Information Commissioner's Office (ICO).This has been further evidenced in the information security incident reported by the council to the ICO this year where training attendance has been a key part of the investigation. This highlights the value to the council of the training programme. There has been slightly reduced attendance on both Social Services and corporate training courses. This reflects the fact that a large number of staff have been trained previously but work is planned out to improve future attendance and provide refresher training. Course evaluation feedback is included in the schools section below and in Appendices A and B.

Social Services Courses

Social Services employees represent a high risk group due to the nature of their business and the information they handle as part of their roles. Of particular note is the information security incident reported to the ICO which related to Social Services. The questions raised by the ICO about this incident further highlight the need for staff training and effective systems to ensure training attendance. This mandatory training has been provided for three years since April 2013. As detailed above this course and the corporate course have been reviewed and standardised to provide greater consistency and flexibility.

In 2015/16 the number of staff attending was 147 which is lower than in 2014/15 (182) and 2013/14 (226). This largely reflects less staff that require training, but does also reflect slight

reductions in attendance. Staff will be reminded of the importance of course attendance and monitoring of course attendance will be carried out by the Information Governance team in conjunction with Social Services.

The part two course provides more detail on information sharing and subject access requests including what information should be redacted (removed) from subject access requests to ensure inappropriate information is not disclosed. This course was not run this year but is planned for the upcoming year. This is tied in to the process for Subject Access Requests and using the Electronic Document Management system for carrying out the redaction.

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated in Appendix B below:-

Corporate Courses

These courses are scheduled on a monthly basis with a maximum of 15 attendees. As detailed in the Social Services section the courses have been combined.

In 2015/16 the number of staff attending the corporate course was 114 compared with 152 in 204/15, 92 in 2013/14 and 57 for 2012/13. This represents a good level of attendance but more can be done to improve this. Work has already commenced targeting senior managers in the Council, regular reminders and checks on attendance will also be carried out.

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated by some analysis in Appendix A below:-

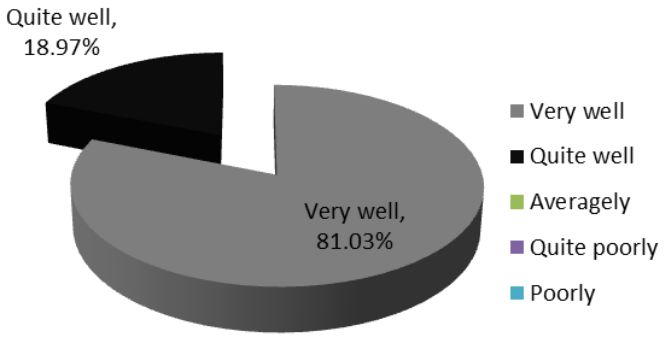
Councillor Courses

Councillor courses took place in 2013/14 and were well received. Courses for councillor have slipped in to the 16/17 financial year and are now scheduled for September2016.

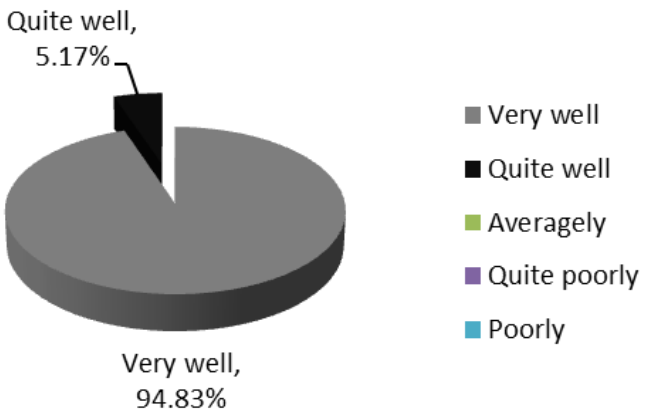
Schools Courses

Specific information security courses for schools were first run in June 2014. This year, four training sessions for schools were held in January/February 2016. As detailed in the organisation section, schools are an important consideration in the council's information governance arrangements so these training sessions show continued commitment to schools. 72 members of staff attended these training sessions in addition to the 63 members of staff who attended training in June 2014. The sessions received positive feedback and analysis is provided below of the feedback forms provided by courses attendees.

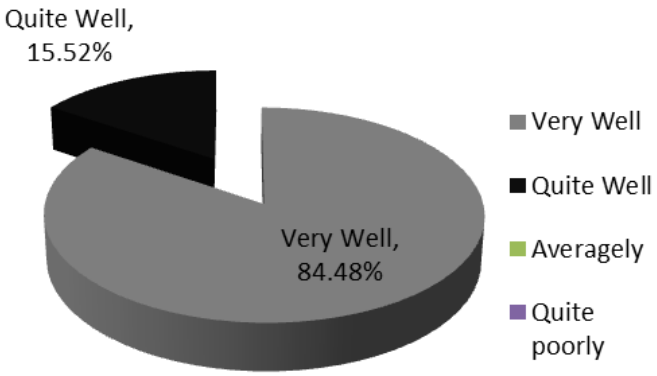
How well were the aims and objectives explained?



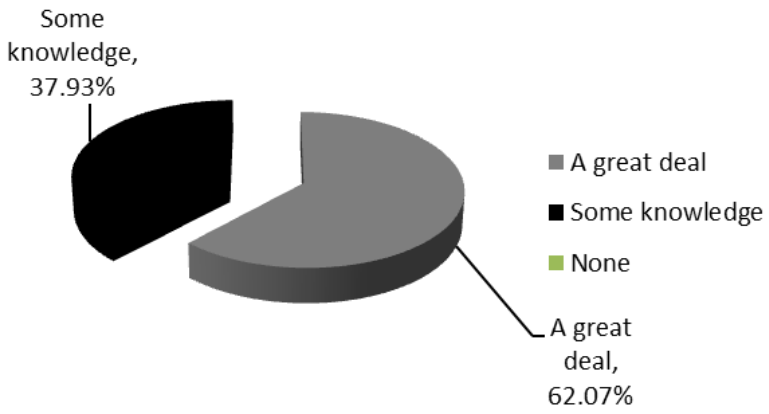
How well did the trainers know their subject?



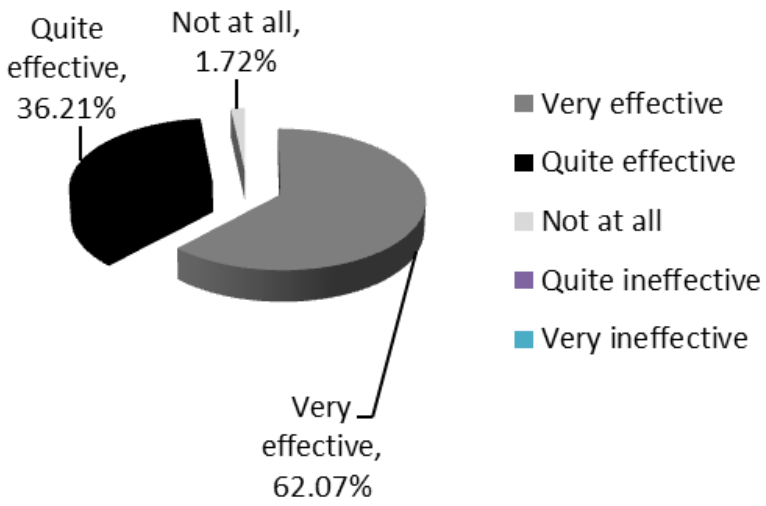
How well did the trainers convey their knowledge?



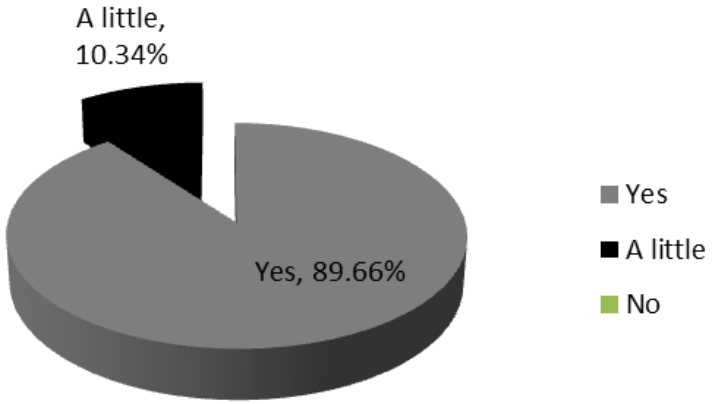
Do you think you learned anything as a result of this course?



How effective were the presentation materials?



Will you be able to apply any new knowledge gained, in your workplace?



Other Courses and Presentations

As well as regular standard training sessions ad hoc sessions are available for specific groups of staff. These tend to be slightly less detailed and designed to highlight key messages. As detailed in previous reports, staff are encouraged to attend standard training courses wherever possible to maximise take up of these sessions and to reduce the resource requirement for ad hoc courses.

In 2015/16 electronic document management training has also been added to the standard training provided by the team, over 100 staff have been trained on the system during 2015/16.

E-Learning

All staff that need access to the council's computer network are required to undertake e-learning before they can access systems. Following a review of e-learning provider, this is now provided on a new system in collaboration with the NHS. This gives staff an appreciation of their obligations in conjunction with a signed form to request access and agree to abide by the council's guidance. Whilst the preference is to provide classroom training, it is recognised that e-learning can be complementary especially to get an initial appreciation. Work has been carried out to review the e-learning content and this is planned to be completed in May 2016.

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. Staff are reminded of these policies where appropriate.

Updated policies

A major review of the Schools IT Security policy was carried out and this has been circulated to schools for adoption.

Policies are also reviewed to ensure that they are still valid and up to date. The following policies have been reviewed and amended over the last year:

Access to the Network, Email and the Internet Policy, Use of the PSN Network and Secure Email Policy, Building Access Policy, Confidential Waste Policy, Disposal of IT Equipment/Mobile Phones policy, Email Policy, Information Security Incident Reporting Policy, Information Retention and Disposal Policy, Information Risk Management Policy, Information Sharing Policy, IT Business Continuity Policy, IT Change Request Policy, System, Access and Development Policy, Telephone and Blackberry Policy, Password Policy, Records Management Policy, Information and IT Security Policy,
Software 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. Policies and guidance to be developed and reviewed in 16/17 include Protective Marking and confidential waste.

2.4. Information Risk Register

As detailed in the information risk management policy, an information risk register is maintained. This identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. The risk register is shared with the Information Governance Group so they are aware of the current status of risks and is maintained by the Information Governance team. The development of the Information Asset Owner and Information Asset Coordinator roles are designed to embed information governance within services and especially effective information risk management.

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. 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. Security Incidents

The Information Security Incident Reporting Policy establishes the requirement for all security incidents to be reported, logged and investigated. Security incidents range from lost phones/other devices and password issues to data breaches where data is lost or passed to the incorrect recipient.

62 security incidents were recorded in 2015/16 compared with 66 in 2014/15, 64 in 2013/14 and 63 in 2012/13. This shows consistency over the last four years. The 62 information security incidents are split in to the categories below as suggested by the ICO, with previous figures shown for comparison:-

Category	2015/16	2014/15	2013/14
Disclosed in error -	23	14	14
Lost or stolen hardware -	12	23	9
Lost or stolen paperwork -	2	0	6
Non secure disposal – paperwork -	0	2	1
Other - non principle 7 incident -	9	18	8
Other - principle 7 (security of personal information) incident -	11	0	4
Technical security failing -	5	9	22
TOTAL	**62**	**66**	**64**

As noted previously, 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 indicative only. There has been an increase in incidents categorised as disclosed in error which tend to be human error. There has been a reduction in lost or stolen hardware. Some of the incidents previously classified as other non principle 7 probably should have been identified as principle 7 in the past so this reflects a more accurate categorisation this year. There has been a further reduction of incidents categorised as technical security failings.

The majority of security incidents recorded were not major concerns and they remain similar year on year, many relating to human error. Some of the themes 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 or blackberries so low risk)
- Lost remote access tokens which present a negligible security risk
- Some personal printed information left on printers internally

The ongoing implementation of EDMS across council services, and move to a new mail solution should support improvements in 2016/17. As staff are now able to access most documents in electronic/ scanned form – and the distribution of mail will be automated as outlined later in the report, reducing risks of handling paper.

The most significant incident this year was reported to the Information Commissioners' Office (ICO). No incidents were reported to the ICO last year. The incident which occurred in Social Services was one of stolen paperwork from an employee's home. This incident was reported to the ICO due to the number of documents being 27 and the sensitivity of the information held in these documents. The other factor influencing reporting was that a council was previously fined £70,000 for a similar incident. However, each case is evaluated by the ICO in its own right taking in to account training and guidance provided and wider the organisational measures to minimise the likelihood of such incidents. The outcome of this report is expected early in 2016/17 and may be reported in later versions of this document.

All information security incidents are investigated and following last year's review the information security incident reporting form gives a background to the incident. Incident reports are compiled following discussion with those involved in the incident. An overview is also reported to the SIRO and Information Governance Group. This work will also be reflected in the risk register and in communications with staff.

2.6. Information Sharing

The drive for more collaborative working across organisations requires that information is shared appropriately. 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 Governance team leads on this work and has developed a number of ISP's with services and other organisations. This work is supported by the information sharing policy developed in 2013/14. A full list of the Council's ISPs is published on the Intranet, the following represents developments in 2015/16:

Information Sharing Protocols (ISP's)

Completed ISP's Awaiting Quality Assurance
Protection of Vulnerable Adults (POVA)
Flying Start

Current and Future Developments
Residential Services
Re-ablement and Care Service
Team around the Cluster
Newport Refugee Practitioners Forum
Families First Prevention and Early Intervention
Anti-Social behaviour, crime and disorder

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 2015/16:
Disclosure of Pupil Information to Support the Schools Vaccination Programme.
Disclosure of Pupil Data Between NCC and Gyrfa Cymru Careers Wales.
Sharing of the Blue Badge Improvement Service (BBIS) data with the Welsh Ministers.
Disclosure of Pupil Information to the Communities First Programme

Further DDA's are being considered in a number of areas.

2.7. Business Continuity

Due to the increasing reliance on information technology to support business activities, the council needs to ensure that activities can operate without access to their systems. In addition, the IT service needs to maximise the availability of the council's IT systems. In 2014/15 priority IT systems were agreed for the first time and are used by the IT Service operationally if issues with systems occur. These systems were reviewed and updated during 2015/16.

As detailed in last year's report, the Wales Audit Office recommended testing a scenario where both server rooms at the Civic Centre are not available to determine how long it will take to set up an offsite server room and what effect this will have on its timetable for restoring its critical systems. A simulation exercise was carried out with IT and the Civil Contingencies Unit. A report summarising the lessons learned and an associated action plan was presented and agreed by the council's Strategic Leadership Team. Good progress on the actions identified in the report

has been made in a number of areas and will be progressed further over the next few months. This will be formally reported back to the council's Strategic Leadership Team shortly.

Work has been completed on systems with a higher than average perceived risk of failure and various infrastructure improvements have been made.

The corporate review of business continuity plans has commenced and IT systems identified in the new plans will be updated and any changes necessary will be made to agreed system priorities.

2.8. Technology Solutions

A number of technical solutions are in place to minimise risk to information and the corporate network generally as outlined below. PSN compliance and the development of business continuity requirements continue to drive technical improvements for information management. Wales Audit Office annually review the controls applied to key financial systems (also reported to Audit Committee).

Mobility solution
The use of a mobility solution has been rolled out for agile workers that 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.

Secure/Large File transfer solution
As identified in last year's report Egress Switch was procured to enable the secure transfer of e-mails and associated documents to organisations and individuals without secure e-mail facilities. This has been rolled out to over 1,500 users to date with implementation to be complete in 2016. 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.

Identity Management
As planned in last year's report, 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 was procured 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. This has commenced roll out with complete roll out planned for 2016. The project has resulted in financial savings, but also reduces information risk.

Bring Your Own Device (BYOD)
The previous BYOD platform was decommissioned on the 4th March 2016, and a new Microsoft solution has been implemented ready for a pilot phase. Feedback relating to governance and security has already been provided to the IT team following tests on smart phones, with further guidance expected in the near future to help formulate a new policy.

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 now represent about 55% of all desktop devices.

Laptops and desktop PCs

- All corporate laptops are protected using an end point protection solution
  - Encryption solution is being changed
  - 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.
- 'Follow Me' print is available to all users, who are able to access Council printers from any location

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.

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 wifi is also now available as part of the 'Digital Newport' work in the city centre (NewportCity Connect) 54 public buildings and on public transport (NewportCommunityCloud). A review of the information used by these systems, and possible accreditation options will take place in 16/17.

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 and part of the development work for 16/17 will be ensuring that the appropriate controls are in place.

Financial Systems

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

2.9. Records Management

Records management continues to develop with the ongoing implementation of the corporate Electronic Document Management System (EDMS) across an increasing number of services. 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 on the EDM system. The project team have worked with each service to understand their business requirements for document management and implemented the solution in 10 service areas between early 2013 and April 2016. The aim is to roll out to the remaining services by March 2017. In June 2015 a pilot system was implemented for payments and went live in November 2015. The project team have delivered training on the system to over 100 staff during April 2015 to March 2016. Education Phase 1 was completed in June 2015 and Phase 2 started in December 2015 and continues. The subject access request file system was implemented in March 2016. There have been numerous developments to existing file systems, including manager access to HR staff records.

For paper documents, work commenced in early 2013 to create a Modern Records facility at the Civic Centre. The room is equipped with racking for the storage of archive paper records. This has been complemented by the acquisition of an IT application to record the location and content of files for retrieval of paper archive documents. By April 2016 about 5,000 boxes of archive documents (over 70% of all centrally stored archive documents) have been migrated to the new facility. The remainder of paper archive documents are in temporary storage within the Civic Centre with the migration of these documents to be completed in 2016/17.

New scanners were purchased to replace older hardware. These new scanners are of a higher specification than previous models due to increased scanning volumes and expected to improve the speed and accuracy of scanning carried out in Document Services, which supports the move to EDMS.

2.10. Freedom of Information and Subject Access Requests

As a public body, 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
Since last year's report the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2015/16 was 914 which shows a slight increase over 14/15 (895). This continues the upward trend of requests year on year. Details of the requests by financial year are detailed below:-

Year	Number of requests
2015/16	914
2014/15	895
2013/14	869
2012/13	698
2011/12	540

Performance for 2015/16 was 92.3% of requests responded to within 20 working days which exceeds the performance indicator target for 2015/16 (87%). This remains a challenge with lots of organisational changes, reducing staff numbers and increased request numbers. During this year an electronic form was added to the council's web site to improve the process for customers

to submit requests. This is now integrated with the FOI request logging system to minimise data entry time and streamline the process.

Publishing data
Government and ICO guidance encourage the publication of data as good practice for public bodies and this is referenced in the publication scheme as part of our commitment to openness and transparency. The transparency page on the Council's website been developed to improve signposting of council data including the continued publication of council spend over £500. During this year, business rates data was also published on the web site. This assists regular requestors with the availability of data on a quarterly basis and is a more open approach to the data we hold. This has also reduced the work required in the service to publish data on request and consequently has been positively viewed within Finance. Plans have been made for the publication of public health funeral data which is now available from April 2016.

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. The only information that should be shared is that specific to the data subject. A new personal information request form was developed during the previous year and this has provided helpful for gathering suitable information to confirm identity when requests are received. Work has been carried out with Social Services who are now using an improved process for logging requests. In addition they are using an improved process for redaction of documents using the EDMS system. This will be expanded to other areas during 2016/17.

3. Risk Management and Associated Action Plan

As detailed in the sections above, a large amount of important work was carried out during 2015/16 led by the Information Governance team in conjunction with services especially IT. The Public Services Network (PSN) accreditation is likely to be more challenging this year due to a higher number of vulnerabilities being identified that the previous year. The incident reported to the ICO places the organisation under greater external scrutiny and it is likely that the ICO will require specific action even if no fine is imposed.

The review by the European Commission of European Data Protection legislation has resulted in an agreed EU Directive with implementation in member states in 2018. One of the main differences is that businesses will be subject to fines up to 4% of annual turnover which is a major increase in possible fines. In addition, mandatory notification of data protection breaches will be required by member states to their data protection authority (the ICO in the UK). The implications of this legislation need to be considered over the next year.

The council has changed its SIRO during the year as part of a review of roles and responsibilities, and the Information Governance Group continues with its important work monitoring risk across services. A significant issue for the next year is the proposal for the council's IT Service to become part of the Shared Resource Service (SRS). This needs to be considered as part of the council's information risk management going forward.

The commitment to information governance remains with on-going training, awareness-raising, policy development, management of security incidents, IT business continuity management etc. Actions identified in this report will be detailed further in the Digital and Information team's business plan.

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	Provision of information security training Staff awareness raising Continue with specific information security training for Social Services Development of new policies and update of existing ones Further improvements to processes for subject access requests	Digital And Information Manager (DAIM) in conjunction with Information Governance 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 Development of Information Asset Register and improved governance arrangements Continued engagement with Members	Digital And Information Manager (DAIM) in conjunction with in conjunction with IT
Proposal for IT service to join Shared Resource Service (SRS)	M	M	Develop relationship with the proposed new service delivery option (SRS)	Digital and Information Manager (DAIM) in conjunction with Head of PBC / SRS management
Preparations for EU General Data Protection Regulations	M	M	Review requirements for new regulations in conjunction with ICO guidance	SIRO
PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	Submission of self-assessment questionnaire and successful compliance achieved Continue technical scanning service to ensure no technical concerns	Digital And Information Manager (DAIM) in conjunction with in conjunction with IT
Technical Solutions are not available to meet the	H	L	Complete roll out of Egress for secure e-mail transfer Roll out of Xerox Mail solution Appropriate actions to support BYOD	IT Infrastructure Manager in conjunction with Digital And Information

needs of service delivery and data breach occurs			Encrypted laptop devices 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	Manager
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 And Information Manager (DAIM) in conjunction with Information Governance team
Critical IT systems are not available to services	H	L	Review and refine priorities for critical IT systems Implement improvements as a result of Disaster Recovery exercise Continue with action plan to improve availability of IT systems Continue with services to develop business continuity arrangements	IT Infrastructure Manager in conjunction with Information Governance Manager and services
Information security is not considered for new projects	M	L	Development and implementation of privacy impact assessments	Information Governance Manager in conjunction with services

3.2 Action Plan

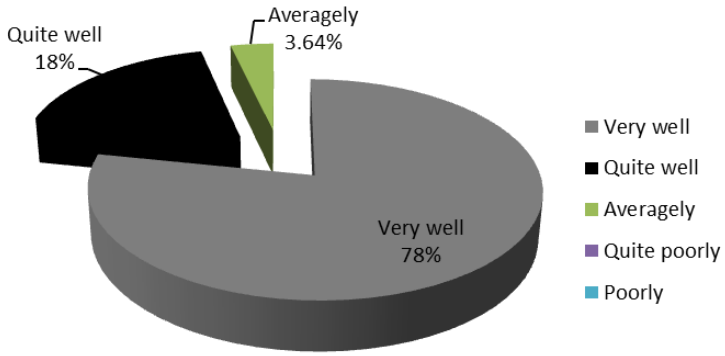
Action	Deadline
Compliance and Audit	
PSN accreditation	
Follow up on remedial action plan to ensure continued PSN compliance	Jun 16
EU General Data Protection Regulation	
Review of the implications of EU General Data Protection Regulations	Dec 16
PCI accreditation	
Payment Card Industry Data Security Standard resubmission or updates as necessary	Feb 17
Follow up actions as a result of the Wales Audit Office review	On-going
Information Governance Culture and Organisation	
Provide feedback to staff following employee survey.	Jun 16
Follow up on actions required as a result of staff comments following	Jul 16

the employee survey.	
Develop relationships with Shared Resource Service if this delivery model for the IT service is implemented as proposed	On-going
Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders	On-going
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Members updated through Annual Information Risk Management Report, including review by Scrutiny Committee.	Jul 16
Formal agreement of Information Asset Owners and creation of Information Asset Register	Jul 16
Communications and Awareness Raising	
Regular information security training sessions corporately and for Social Services including revision of content as necessary	On-going
Target senior managers for Data Protection training.	May 16
Provide regular reminders and checks on attendance corporately and in Social Services	Sep 16/ On-going
Review and deliver Part 2 training course for relevant Social Services staff	Jul 16
Provide information security training courses for councillors as provided last year	Jun 16
Complete review of Protective Marking policy.	Jun 16
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 – including confidential waste.	On-going
Provide advice and guidance to support schools with the Education service. Development of policies to support schools.	On-going
Complete review of e-learning provision and re-publish	May 16
Information Risk Register	
Management of the information risk register	On-going
Security Incidents	
Investigation of security incidents and identification of issues to be followed up	On-going
Review findings from incident referred to ICO and take appropriate actions as a result	Jul 16
Information Sharing	
Further Information Sharing Protocols will be developed to support collaborative working	On-going
Review existing Information Sharing Protocols	On-going
Finalise Data Disclosure Agreement for Communities First	Jun 16
Develop additional Data Disclosure Agreements as required	On-going
Business Continuity	
Make disaster recovery/business continuity improvements as a result of WAO.	Dec 15
Continue the action plan identified in the IT systems business continuity report including refining an updating priority IT systems	On-going

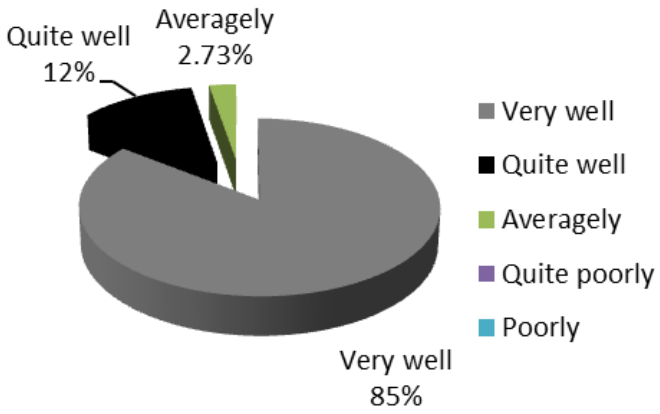
Technology Solutions	
Complete roll out of Egress solution across the council	Dec 2016
Improve communications and guidance to support the roll out of Egress	May 16
Roll out of Xerox Mail solution to improve mail distribution processes	Jul 16
Review and roll out of BYOD solution as appropriate	Jul 16
Consider options and controls required for cloud-based systems where appropriate	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
Completion of Modern Records facility	Dec 16
Review of resources supporting EDMS project	Dec 16
Freedom of Information and Subject Access Requests	
Freedom Of Information	
Publication of public health funeral data set on council web site	Apr 16
Publication of further open data for suitable data sets	On-going
Subject Access Requests	
Roll out of EDMS solution for redaction of Subject Access Requests	Sep 16
Roll out of FOI request system for managing Subject Access Requests	Sep 16
New projects	
Review public wifi provision and information collection	Jun 16

Appendix A. Corporate Information Security Training Evaluation Feedback.
110 Staff trained over 12 courses 2015-16

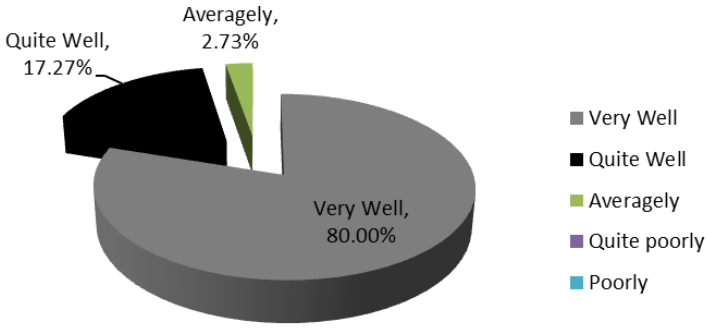
How well were the aims and objectives explained?



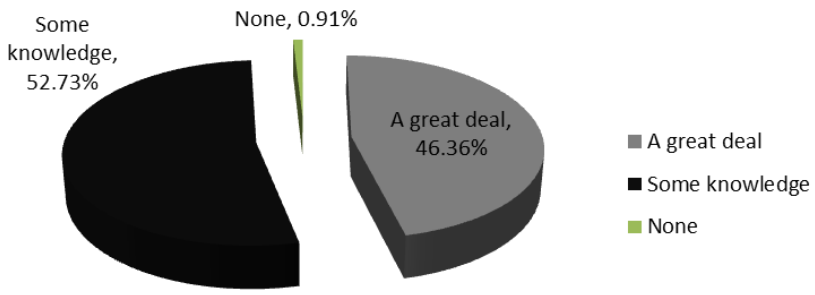
How well did the trainers know the subject?



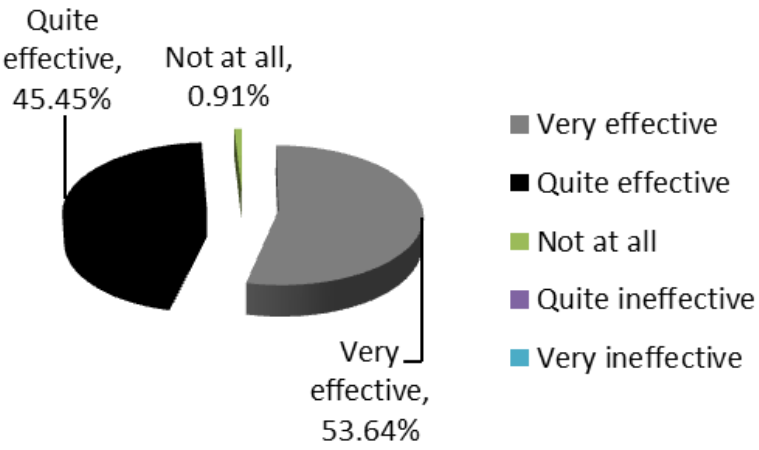
How well did the trainers convey their knowledge?



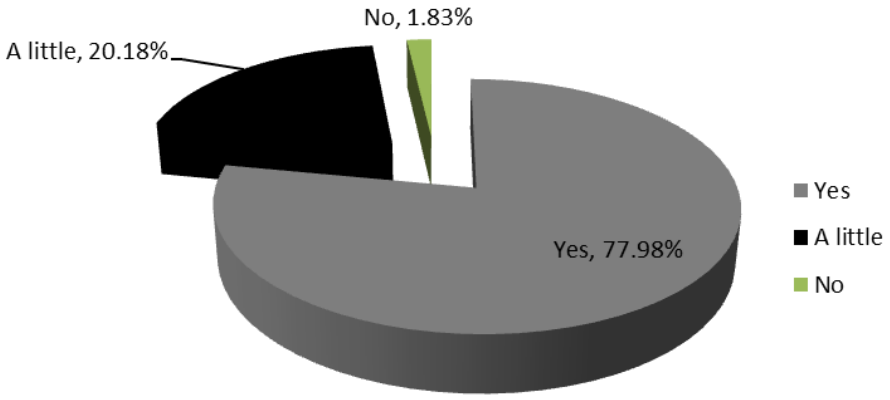
Do you think you learned anything as a result of this course?



How effective were the presentation materials?

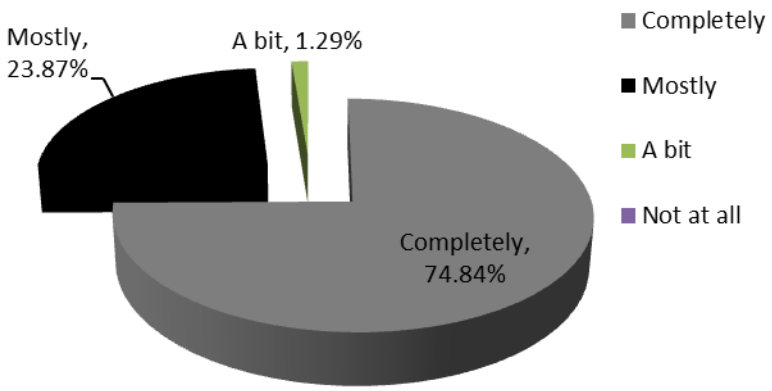


Will you be able to apply any new knowledge gained, in your workplace?

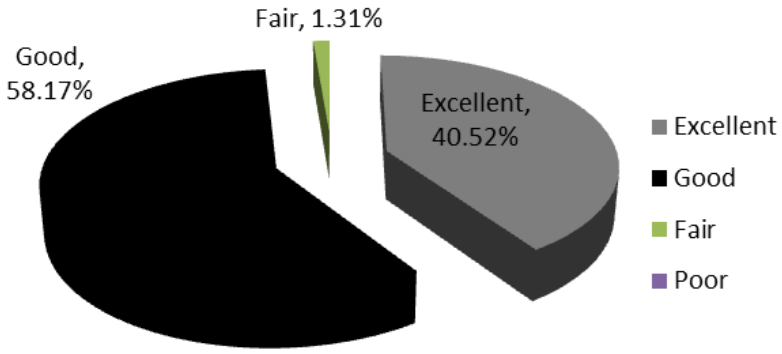


Appendix B. Social Services Data protection Training Evaluation Feedback.
155 Staff trained over 15 courses 2015-16

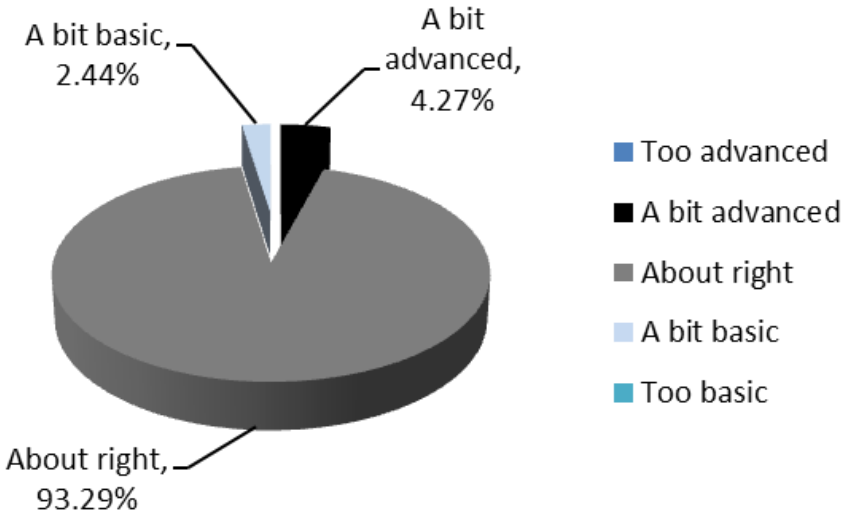
The agreed objectives were met:



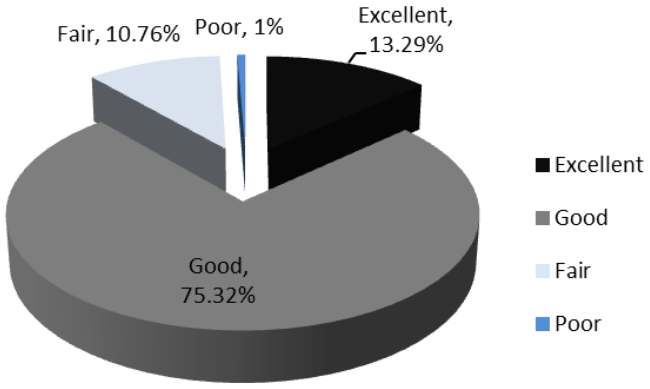
The standard of presentation was:



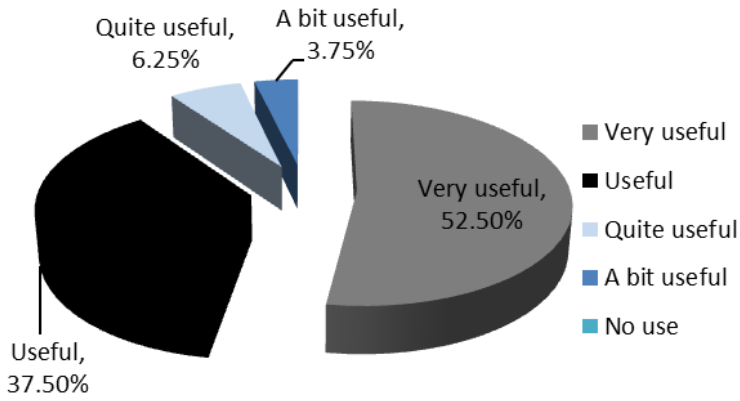
The level of training was:



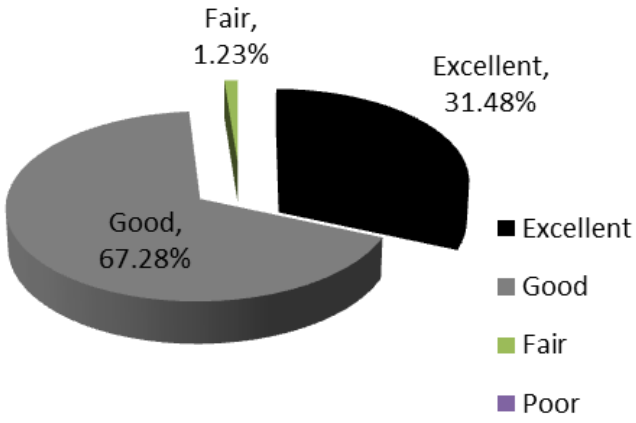
The standard of the venue and facilities were:



How useful has this training been for the work that you do?



Overall I considered the training to be:



Would you recommend that other colleagues attend this training?