QAH
QUEEN ALEXANDRA Hospital

Portsmouth Hospitals NHS
NHS Trust

Information Risk Management

Senior Information Risk Owner

Annual Report 2014/15

Peter Mellor
Director of Corporate Affairs and Business Development | Senior Information Risk Owner (SIRO)
Information Risk Management Annual Report 2013-14

May 2014

Executive Summary

The Senior Information Risk Owner has responsibility for ensuring organisational information risk is properly identified and managed, and that appropriate assurance mechanisms are in place.

The purpose of this Annual Report is to provide assurance of practice, progress and developments in Information Risk Management, particularly in relation to relevant standards of the NHS Information Governance Toolkit.

The Trust compares well against local provider trusts and (nationwide) comparable provider trusts in its Information Governance Toolkit performance. Compliance with the Information Governance Toolkit training target was a significant achievement in 2013/14, although sustaining this presents a similar challenge for the year ahead.

There continues to be an improvement in the awareness of, and progress with, information risk requirements in this financial year. However, there are pockets of poorer compliance / assurance, generally within those CSCs that have struggled for continuity with their operational and business management roles. Often, their information governance focus suffers as a result.

Sufficient assurance of information risk management practices does require staff at a local level to develop their knowledge of the Information Governance Compliance Framework (the Trust's compliance monitoring and assessment tool) and this can take time to achieve. Changes to those staff members with information governance responsibilities will adversely affect this.

The Trust was required to report one data protection incident to the Department of Health and Information Commissioner's Office in 2013/14. The Trust was investigated by the Information Commissioner's Office and, whilst the Trust was found to have failed to comply with the Data Protection Act, no further regulatory action was taken.

The NHS remains the industry reporting the highest number of data protection breaches. Mandatory breach reporting does not currently exist for the private sector but this may change when new EU data protection reforms are introduced some time in the next two years.

The very nature of information risk management means that existing good practice must be maintained in order to provide the Trust with an appropriate level of assurance in the currently intense and high-scrutiny information governance environment.

1. Introduction

1.1. Following the high profile loss of 25 million child benefit records by HM Revenue and Customs in November 2007 and the Government's Data Handling Review, Government Departments were required to implement an accountability framework, which included the identification of a Senior Information Risk Owner (as senior manager within an organisation with Board level responsibilities).

1.2. The Senior Information Risk Owner has responsibility for ensuring organisational information risk is properly identified and managed and that appropriate assurance mechanisms are in place. They should be familiar with risk management and the organisation's response to risk.

1.3. The role of the Senior Information Risk Owner is to "take ownership of the Trust's Information Risk Policy, act as advocate for information risk at the Board and provide written advice on the Annual Governance Statement in regard to information risk".

1.4. The role of Senior Information Risk Owner was assigned to the Trust's Company Secretary in 2008. The role compliments, but should not be confused with, the Trust's Caldicott Guardian (Medical Director) who is responsible for the confidentiality of patient information and acts as the "conscience" of the organisation in this respect.

2. Purpose

2.1. The purpose of this report is to provide assurance of practice, progress and developments in Information Risk Management, particularly in relation to relevant standards of the NHS Information Governance Toolkit.

2.2. The aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise, and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

2.3. The purpose and format of this Annual Report may evolve in response to external influences such as the NHS Information Governance Toolkit, examples of Data Protection enforcement (Financial Penalty Notices) and also the assurance requirements and expectations of the Trust Board.

3. Management

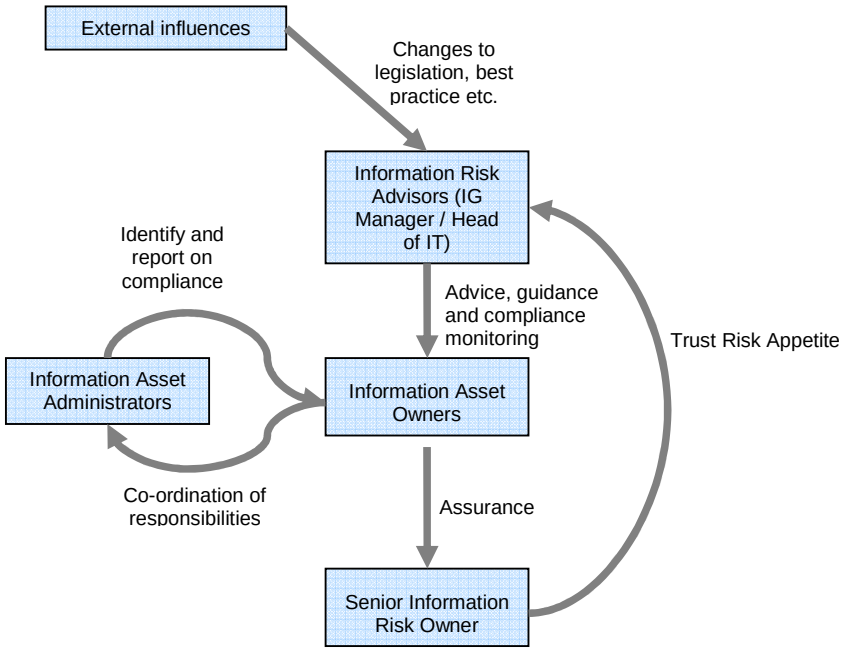
3.1. The Senior Information Risk Owner has been supported in an advisory capacity by an informal Information Risk Management Group (including the Head of IT and Information Governance Manager). Formally, the Senior Information Risk Owner is supported by a network of Information Asset Owners (IAO) within each Clinical Service Centre and

Corporate Function, who are responsible for addressing information risks locally, reporting and providing assurance to the Senior Information Risk Owner.

3.2. All Clinical Service Centres are required to report biannually to the Trust's Information Governance Steering Group (IGSG) on their compliance against relevant information governance requirements (which includes information risk management). The Senior Information Risk Owner attends these meetings.

3.3. Information Asset Owners have also been required to report annually, directly to the Senior Information Risk Owner, relating specifically to information risk management.

3.4. Overview of the Information Risk Management assurance process:



4. Scope

4.1. Information risk management may be inherent in a wide variety of information governance initiatives, but the work with Information Asset Owners has focussed on a core group:

- Information Governance Training
- Information Asset Registers
- Flow Mapping Registers
- Information Governance Incidents
- Information Governance Contractual Clauses

4.2. The significance of information risk management can be demonstrated with reference to four of the six Strategic Objectives within the Trust's current Information Governance Strategy (2015-17):

- Continue to achieve 'Satisfactory' compliance with the NHS Information Governance Toolkit
- Promote responsible, patient-centred information sharing in line with the principle recommendations of the Caldicott 2: Information Governance Review
- Identify and reduce information risks and reduce the potential impact of information governance incidents
- Promote a culture of openness and transparency in line with the spirit of the Freedom of Information Act and the Government's Transparency Agenda
- Understand the implications and prepare for the impact of changes to EU Data Protection legislation
- Promote the principles of Privacy by Design and embed a culture that understands the value of early privacy assessment in the project / change cycle

4.3. The Trust's completion of the NHS Information Governance Toolkit provides an assessment of information governance compliance (against central expectations) and a comparison against the compliance of other NHS organisations. Information risk management is relevant to multiple standards of the Information Governance Toolkit.

4.4. Local Provider Trusts Comparison

Pos.	Provider Trust	2014/15 % Score	2013/14	2012/13	2011/12	Change from 13/14
1	Oxford University Hospitals NHS Trust	91%	86%	81%	71%	+5%
2	Isle of Wight NHS Trust	86%	86%	82%	74%	0%
3	Portsmouth Hospitals NHS Trust	85%	86%	85%	75%	-1%
	Salisbury NHS Foundation Trust	85%	81%	83%	85%	+4%
5	Milton Keynes General Hospital NHS Trust	84%	88%	85%	81%	-4%
6	Oxford Health NHS FT	82%	90%	82%	80%	-8%
	Southern Health NHS FT	82%	80%	75%	73%	+2%
8	Buckinghamshire Healthcare NHS Trust	80%	76%	75%	73%	+4%
	Royal Berkshire NHS FT	80%	77%	78%	76%	+3%
10	Solent NHS Trust	77%	75%	80%	63%	+2%
11	Hampshire Hospitals NHS FT	76%	71%	68%	65%	+5%
12	Frimley Health NHS Foundation Trust	73%	75%	76%	74%	-2%
13	South Central Ambulance Service NHS Trust	71%	83%	79%	76%	-8%
	University Hospital Southampton NHS FT	71%	71%	72%	71%	0%
15	Berkshire Healthcare NHS FT	66%	68%	67%	68%	-2%

4.5. Comparable Acute Trusts (based on CQC Intelligent Monitoring and Friends and Family Test benchmarking)

Pos.	Provider Trust	2014/15 % Score	2013/14 % Score	2012/13	2011/12	Change from 13/14
1	City Hospitals Sunderland NHS FT (FFT)	86%	86%	84%	83%	0%
2	Portsmouth Hospitals NHS Trust	85%	86%	85%	75%	-1%
3	Derby Hospitals NHS FT (FFT)	81%	77%	77%	72%	+4%
4	South Tees Hospitals NHS Trust (CQC IM)	80%	82%	74%	73%	-2%
	Royal Berkshire NHS FT (CQC IM)	80%	77%	78%	76%	+3%
6	Norfolk & Norwich Uni. Hosp. NHS FT (FFT)	74%	74%	68%	68%	0%
	Bolton NHS FT (FFT)	74%	68%	68%	63%	+6%
	Maidstone and Tun. Wells NHS Trust (CQC IM)	74%	82%	80%	74%	-8%
9	Royal Cornwall Hospitals NHS Trust (CQC IM)	73%	72%	72%	68%	+1%
10	Hull & East Yorks Hosp. NHS Trust (CQC IM)	71%	71%	74%	71%	0%
	University Hospitals Southampton NHS FT (FFT)	71%	71%	72%	71%	0%

4.6. The Trust decreased in compliance from 86% in 2013/14 to 85%, but retained the level required for 'Satisfactory' compliance. This requires a minimum of level 2 attainment for all 45 standards. The "Satisfactory" outcome is the primary indicator of compliance and was therefore the focus in 2014/15.

4.7. Nationally, the Trust ranked 20th out of 156 acute trusts.

5. Measures

5.1. Since a major revision to the NHS Information Governance Toolkit in 2010/11 the Trust has assessed compliance with Toolkit standards at a local level (i.e. by Clinical Service Centre and Corporate Department) when previously they were only assessed centrally. This is in order to satisfy the revised requirement to provide more comprehensive evidence and assurance of compliance.

5.2. This has resulted in a much deeper understanding of practice and performance, but as a consequence has also unearthed areas of non-compliance and naturally becomes a larger structure to govern.

5.3. An Information Governance Compliance Framework has been developed to help communicate these local requirements, and is used to monitor and assess compliance at a local level. The Compliance Framework covers between 10 and 15 relevant requirements depending on the Clinical Service Centre / Corporate Department's operations.

5.4. For Information Risk requirements, the Information Governance Compliance Framework focuses on the five areas identified in section 4.1.

5.5. The requirements can be summarised as:

- **Contracts (Information Governance Toolkit Standard 110)** – formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.

  What we have found: whilst the contract templates available through the formal Procurement process largely satisfy this requirement, many contracts appear to have been arranged and negotiated at a local level and contain insufficient clauses, providing insufficient assurance. Some contracts have proved difficult to physically locate and often only one paper copy is held.

  What is the information risk: clauses can set out the expected data protection practices of third parties, ensure the Trust is made aware of incidents at the earliest opportunity and can indemnify the Trust in cases of data loss caused by the third party.

  What does "compliance" look like? All relevant contracts have been identified and assessed and review dates for weak / deficient contracts have been confirmed.

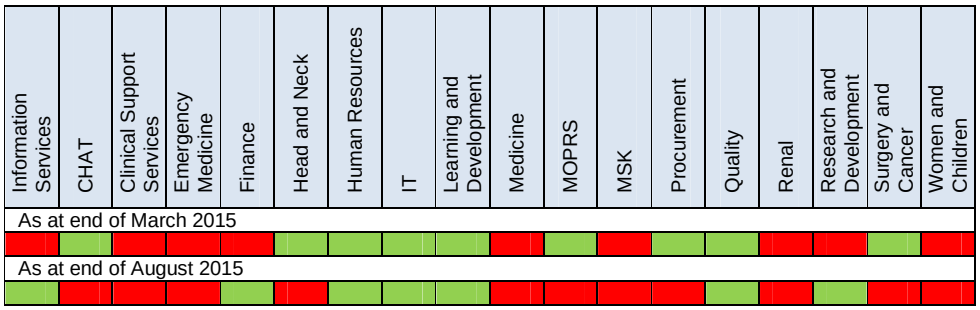
Information Services	CHAT	Clinical Support Services	Emergency Medicine	Finance	Head and Neck	Human Resources	IT	Learning and Development	Medicine	MOPRS	MSK	Procurement	Quality	Renal	Research and Development	Surgery and Cancer	Women and Children

- **Staff Training (Standard 112)** – information governance awareness and mandatory training procedures are in place and all staff members (95%) are appropriately trained.

  What we have found: the Trust-wide use of the Essential Skills Handbook, as well as ongoing promotion of the information governance training target, has helped improve and maintain information governance training rates throughout the year. However, consistent achievement of a 95% training rate still presents a particular challenge.

  What is the information risk: there is a greater risk of information governance / data protection incidents as a result of an untrained workforce. Training is seen as a key corporate defence in the event of a data protection incident.

  What does "compliance" look like? 95% of staff members have their Information Governance training competency (annual basis).



- **Information Asset Register (Standard 307)** – all key information assets have been identified and regular risk reviews are undertaken

  What we have found: responsibilities for Information Assets (usually these are administration systems or databases) are not routinely updated and many 'responsible' staff members are no longer in relevant posts. There has been a failure to engage in the risk management process in some Clinical Services Centre, which risks the inappropriate management of sensitive data and a proliferation of data protection incidents.

  What is the information risk: a number of un-governed information assets introduces a wide range of information risks from insecure practices; could be seen as a breach of the Data Protection Act (holding minimum necessary data, for the minimum necessary length of time); has the potential for significant incidents (as databases generally hold data on very large numbers of individuals); and could introduce clinical risk through poor data quality (e.g. from standalone databases that become out of date)

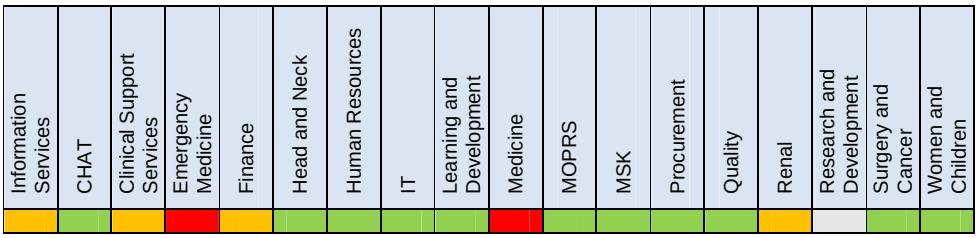
  What does "compliance" look like? Assurance that all assets have been identified, all relevant staff members have completed Information Risk Management training, and risk assessments have been completed for all Information Assets.

- **Flow Mapping Register (Standard 308)** – all transfers (of hardcopy and digital personal identifiable and sensitive information) have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.

  What we have found: there is still some variation in completion of Flow Mapping Registers (records of what information is transferred, why it is transferred, and how it is transferred), but generally engagement with this requirement is improving. Flow Mapping Registers were introduced primarily to identify and mitigate the risks associated with unencrypted transfers of personal data and have been largely successful in this regard, although they are limited to routine transfers of personal data and therefore cannot provide assurance of all (i.e. ad hoc) arrangements, which rely on the awareness of staff.

  What is the information risk: misdirection of confidential information as a result of poor or inappropriate practice, such as breaches resulting from using inaccurate fax numbers, misaddressed e-mails or post. The misdirection of single documents presents the most likely risk of a medium-severe breach.

  What does "compliance" look like? Flow Mapping Registers are accurate, complete and up to date (reviewed within last 12 months at most).



- **Information Governance Incidents**

  What we have found: information governance incidents can be considered as a very broad category, which makes effective comparisons difficult. Relevant incidents could include mislabelled specimens and samples, failing to note relevant information in a patient record or failing to communicate information effectively with a patient. More 'obvious' incidents include data losses and other direct forms of breaches of confidentiality such as misdirecting confidential mail. The most common (medium – high risk) incidents over the last few years relate to the misplacement / loss of handover sheets / patient lists both onsite and offsite, the misdirection of patient letters (incorrect recipients), and misfiled documents in patient records.

  What is the information risk: these incidents are effectively the outcomes of our information risks. The Trust must adhere to the Department of Health guidance on managing information governance incidents, which has its own grading system. Depending on the severity of incident, there may be a need to report it to the Department of Health and the Information Commissioner's Office.

  What does "compliance" look like? There should be assurance that staff members know how to recognise and report an information governance incident. Incidents must be investigated appropriately and lessons learned / recommendations should be identified and communicated appropriately.

Information Services	CHAT	Clinical Support Services	Emergency Medicine	Finance	Head and Neck	Human Resources	IT	Learning and Development	Medicine	MOPRS	MSK	Procurement	Quality	Renal	Research and Development	Surgery and Cancer	Women and Children

Grey indicates that the requirement is generally not applicable, as there have been no incidents experienced over a lengthy period of time, and there are no data / trends to analyse.

6. Summary of Information Risks

Information Governance Incidents

- Local governance of incidents (reporting, investigation and learning)
- Difficult to undertake analysis over time due to changes in reporting guidance and introduction of DatixWeb
- Management of paper records (especially handover sheets)
- Data quality (e.g. mixed addresses) or admin errors leading to misdirected mail

Data Transfers

- Flow Mapping Registers are generally complete and up to date
- No recorded Red Risks
- Some records may be inconsistent with actual practice (e.g. fax)
- Some areas with very low record of their practice

Information Asset Registers

- More around best practice than an immediate, operational risk
- Provide the foundation for many other IG requirements
- Some CSCs still have very sparsely completed registers

Training

- Compliance achieved against a very challenging target
- Similar effort will be required in 2015/16 to ensure 95% competency

Contracts

- Improving awareness of the need for information governance clauses in contracts
- Many contracts in place are not based on Procurement templates, although this is reducing
- Contracts are often not easily retrieved, reviewed and amended

7. Information Governance Incidents

2014/15	Severity					Total
	Near Miss	Green	Yellow	Amber	Red	
Quarter 1	29	52	15	6	0	102
Quarter 2	24	83	10	4	2	123
Quarter 3	26	66	13	3	0	108
Quarter 4	31	73	15	5	0	124
Total	110	274	53	18	2	457

7.1. NHS guidance on the management and investigation of information governance incidents requires NHS organisations to report incidents of a certain severity to the Information Commissioner's Office and the Department of Health. Externally reportable incidents are determined by the relevance of certain "sensitivity factors" to the incident.

7.2. Tightening of Department of Health guidance (in November 2014) relating to external reporting requirements means that the Trust's internal grading may be affected as a result. There could be an increase in incidents graded as Yellow, Amber or Red against the Trust grading scale.

7.3. There have been two Red incidents in 2014/15, one of which was reported to the Information Commissioner's Office / Department of Health. The other incident was graded Red more as a result of staff behavioural issues than the extent of the confidentiality breach. The Information Commissioner's Office investigated the Trust and determined that, whilst the Trust had failed to comply with the Data Protection Act, no further regulatory action was to be taken.

7.4. The number of Yellow and Amber incidents remains comparable to previous years. From 2010/11 to 2014/15 there has been significant variation in the total reported information governance incidents.

Incident Date	Severity					Total
	Near Miss	Green	Yellow	Amber	Red	
2010/11	155	423	19	8	2	607
2011/12	239	566	51	10	4	870
2012/13	53	160	28	12	0	253
2013/14	109	218	37	8	0	372
2014/15	110	274	53	18	2	457

7.5. Between February 2012 and January 2013 the Trust introduced the online incident reporting system DatixWeb. The introduction of a new electronic reporting system was expected to impact on reporting levels until staff became familiar with the new process. Changes to reporting rates in other trusts suggested that the reduction would be around 25%, but also that reporting rates would return to normal levels after around 12 months.

7.6. At a Trust-wide level, the number of reported Information Governance incidents fell from 870 in 2011/12 to 253 in 2012/13. This was a reduction of 70.9%, significantly more than had been expected, and could either be attributed to a genuine reduction in the number of Information Governance incidents, or because there was something about certain (presumably lower severity) Information Governance incidents that made them more likely to have gone unreported in 2012/13.

7.7. Between 2012/13 and 2013/14 there was a 47.0% increase in the number of reported Information Governance incidents – up to 372 incidents. In 2014/15 the figure rose to 457 – an increase of 22.8% – from 372.

7.8. Speculatively, certain milestones may have influenced the apparent lack of consistency in (reporting of) incident numbers:

- In **November 2007** there was a high profile national data protection incident, which resulted in immediate media / regulatory scrutiny and an increased awareness of potential data protection incidents and the importance of incident reporting
- In **January 2010** the Department of Health introduced new Information Governance Incident Reporting Guidance, which would have become increasingly established leading up to February 2012
- In **February 2012** the Trust began the phased introduction of a new electronic incident reporting system DatixWeb, which resulted in a drop of reported incidents
- In **November 2014** the Department of Health introduced a new version of the Information Governance Incident Report Guidance, which has placed lower thresholds on incident types that require externally reporting and which, from April 2015, will affect the internal grading of medium – high severity Trust Information Governance incidents

7.9. Fundamental principles of information risk management can not only reduce the likelihood of an incident but also provide corporate defence in event of one. Important factors include:

- If an individual was responsible for causing an incident, had they received training on data protection?
- Was the incident the result of a failure to adhere to clear, expected best practice (e.g. encryption or secure e-mail)?
- Was the organisation aware of a particular risk, but failed to take adequate steps to address and reduce it?
- Has the organisation experienced a similar incident in the past which would suggest that it appeared not to have learnt any lessons from it?

8. National Data Protection Incidents

8.1. Currently, mandatory reporting requirements are limited to public sector organisations and telecoms providers (introduced from 25 August 2013). This is a likely cause of the majority of fines being made against healthcare bodies and local councils. The EU-wide data protection reforms currently being drafted are likely to see mandatory breach reporting for all industries and could affected trends in enforcement action.

8.2. The health sector still makes up the most significant proportion of all incidents reported to the Information Commissioner's Office. However, health and council organisations have not received Monetary Penalty Notices in the same volume or proportion as previous years. The most significant fines still relate to the mishandling of / failure to secure personal data, but the majority of Monetary Penalty Notices are now for privacy intrusions (breaches of the Privacy and Electronic Communications (PEC) Regulations) related to unsolicited marketing and nuisance calls.

8.3. The following table is taken from the Information Commissioner's Office incident statistics for 2014/15.

Data Breach Incidents by Quarter 2014-15					
Sector	Q1	Q2	Q3	Q4	Total
Accountants	1	2	4	3	10

Audit / Inspections	1	0	0	0	1
Central government	11	6	9	9	35
Charities	9	14	27	26	76
Clubs / Associations	6	6	3	3	18
Courts / Justice	3	2	2	1	8
Credit reference	1	1	0	1	3
Debt collectors	1	1	3	3	8
Direct marketing	0	6	0	1	7
Education	39	21	34	35	129
Estate agents	0	3	3	2	8
Financial advisers	13	7	4	5	29
General business	34	28	13	16	91
Health	183	196	184	184	747
Housing	15	11	16	8	50
HR matters	0	0	0	1	1
Insurance	6	5	5	5	21
Internet	3	4	0	4	11
Leisure	0	1	4	0	5
Lenders	15	11	14	13	53
Local Government	62	55	67	49	233
Mail order	0	0	0	0	0
Media	0	2	2	1	5
Motor industry	0	0	0	4	4
MPs	0	0	0	1	1
Other	2	5	6	9	22
Other individuals	0	0	0	0	0
Pensions	3	1	1	1	6
Police and criminal records	10	12	8	19	49
Political parties	2	0	0	0	2
Prisons	0	0	0	0	0
Probation	0	0	0	0	0
Professional associations	0	1	0	0	1
Recruitment agencies	4	3	4	1	12
Regulators	1	2	5	7	15
Religious organisations	1	1	0	2	4
Retail	5	1	8	6	20
Social services	8	0	2	3	13
Solicitors / Barristers	14	17	31	20	82
Telecoms	5	2	3	7	17
Tenancy	0	0	0	0	0
Travel	1	1	3	7	12
Utilities	0	1	2	2	5
Total	459	429	467	459	1,814

8.4. Monetary Penalties 2014/15

Month	Organisation Type	Fine	Cause
April 2014	Commercial Business	£50,000	Unsolicited Marketing
July 2014	Commercial Business	£150,000	Website Hacked
July 2014	Commercial Business	£50,000	Unsolicited Marketing
August 2014	Government Department	£180,000	Mishandling Information
October 2014	Commercial Business	£70,000	Unsolicited Marketing
November 2014	Commercial Business	£7,500	Website Hacked
December 2014	Commercial Business	£70,000	Unsolicited Marketing

December 2014	Telecommunications	£1,000	Failing to Report a Breach
December 2014	Commercial Business	£90,000	Nuisance Calls
February 2015	Commercial Business	£175,000	Website Hacked
March 2015	Government Department	£180,000	Accidental Disclosure

8.5. Summary of Monetary Penalties since enforcement powers began in April 2010

Year	Number of Monetary Penalty Notices [1]	Average Monetary Penalty [2]
2014/15	11	£115,500
2013/14	17	£158,000
2012/13	22	£130,000
2011/12	10	£86,000
2010/11	4	£78,000

[1] Including penalties for breaching the Privacy and Electronic Communications (PEC) Regulations 2003
[2] Not including penalties for breaching the Privacy and Electronic Communications (PEC) Regulations 2003