South Tees Hospitals NHS
NHS Foundation Trust

Agenda Item Number 10.1

Meeting / committee:	Board of Directors	**Meeting date:**	31st July 2012

This paper is for: (Only 1 column to be marked with x as appropriate)	Action/Decision	Assurance x	Information

Title:	Information Governance Annual Report

Purpose:	This report is to inform the Board of Directors of progress against the Information Governance (IG) work programme in 2011/12 and to outline the key priorities and associated work programmes for 2012/13.

Summary:	The Paper provides information on the: • Progress made in 2011/12 • High Level Project Plan for 2012/13 (Appendix B) • Proposed submission for the Information Governance Toolkit baseline score for July 2012 (Appendix C)

Prepared by:	Nicky Huntley Head of Information Governance	**Presented by:**	Joanne Dewar IT & Health Records Director

Recommendation:	The Board of Directors is asked to: • note the progress against the information governance action plan for 2011/12 • agree the key priorities for 2012/13 • approve the July submission of the baseline score for the IG Toolkit

Implications (please mark an X)	Legal X	Financial X	Safety & Quality X	Strategic X	Risk & Assurance X

Agenda Item Number 10.1

South Tees Hospitals NHS Foundation Trust

Information Governance Annual Report 2012/13

1. Introduction

1.1 The purpose of this report is to confirm the Trust's progress within the Information Governance Assurance Framework for 2011/12 and to set out the key areas of work for 2012/13.

1.2 A Glossary is attached at Appendix A.

2. Background

2.1 Information Governance (IG) is the way by which an organisation handles all of its information, in particular its personal and sensitive information. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, ethically and efficiently in order to deliver the best possible care.

2.2 Information Governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of information and has four fundamental aims:

i) To support the provision of high quality care by promoting the effective and appropriate use of information.

ii) To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.

iii) To develop support arrangements and provide staff with appropriate tools and support to enable then to discharge their responsibilities to consistently high standards.

iv) To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

2.3 The Information Governance Department currently consists of the following:

- Head of Information Governance
- Deputy Information Governance Manager
- IG Specialist – Freedom of Information & Records Management
- IG Specialist - Data Protection & Compliance
- IG Specialist - Registration Authority Manager
- IG Officer
- IG Trainer – temporary position until April 2013
- Secretarial support (shared with the ICT service)

2.4 In June 2010 The Trust appointed Professor Rob Wilson as Caldicott Guardian. The Caldicott Guardian is a senior person within an organisation who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

2.6 The Trust currently has an Information Governance Steering Group to provide advice and assurance to the Trust on all matters concerning information governance. The group is chaired by the Director of IT & Health Records as the Senior Information Risk Owner (SIRO) and authorised by the Formal Management Group to fulfil its duties and make recommendations within its terms of reference.

2.7 Each division/directorate is required to have a representative at the Data Quality and Information Governance Forum. The forum deals with operational issues and concerns regarding data quality and information governance and acts as a vehicle for training and awareness sessions for representatives to feedback within their divisions/directorates. The Data Quality & IG Forum reports to the Information Governance Steering Group.

3. Legislation, National Standards & Policy

3.1. Legal & Professional Obligations

3.1.1 There is a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly a range of statutes that permit or require information to be used or disclosed. The Department of Health has now produced ***NHS Information Governance – guidance on legal and professional obligations***, a best practice guidance document which outlines the likely impact of these provisions primarily on NHS information, but it also includes some social care information. The requirements of the Freedom of Information Act 2000, Data Protection Act 1998 and Human Rights Act 1998 (Article 8 – privacy) are incorporated into the IG Framework.

3.1.2 Presently the most commonly dependent legislation, guidance and national standards around Information Governance are:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- IG Toolkit
- NHS Information Governance Statement of Compliance
- NHS Information Risk Management
- International Standard for Information Security: ISO/IEC 27002:2005
- Care Quality Commission
- NHS Operating Framework
- NHS Quality Accounts
- Connecting for Health/National Programme for IT
- NHS Code of Practice: Confidentiality
- NHS Code of Practice: Records Management
- NHS Code of Practice: Information Security Management

3.2 Information Commissioner's Office - Data Protection Notification Changes

3.2.1 The Information Commissioners Office (ICO) maintains a public register of data controllers (notification). Each register entry includes the name and address of the data controller and a general description of the processing of personal information by a data controller. A data controller must inform the ICO of any changes as soon as possible and in any event within 28 days. Failure to keep a register entry up to date is a criminal offence. South Tees Hospitals NHS Foundation Trust Data Protection Notification has been updated to reflect the transfers outside of the European Economic Area for the following purposes:

- Health Administration and Services - the provision of patient care and administration of health care services in NHS hospitals or community services or family practice
- Public Health - Prevention and control of disease within the community and wider areas.

3.3 Information Commissioner's Office – New Powers

3.3.1 On the 24th April 2012 the first monetary penalty notice to an NHS organisation for breaching the Data Protection Act was served after sensitive data about a patient was released to the wrong person. The NHS organisation responsible will have to pay a £70,000 penalty. A number or monetary penalties have been issued since, the latest on the 19th June 2012 to Belfast Health and Social Care Trust for £225,000 following a serious breach of the Data Protection Act. The breach led to the sensitive personal data of thousands of patients and staff being compromised due to lack of records management during transition of sites and services. The Trust also failed to report the incident to the ICO.

3.3.2 The Information Commissioner's head of enforcement said: “The health service holds some of the most sensitive information available. The report that was sent contained explicit details relating to the patient's health and represented a serious breach of the Data Protection Act”.

3.3.3 As a data controller the trust has a legal obligation under the Data Protection Act 1998 to protect and keep secure all of the information it comes in to contact with in the course of providing its services to the public.

3.3.4 Security issues and data breaches are always high profile and the IG Department has seen an increase in their involvement in the number of informal complaints around breaches/potential breaches of confidentiality has increased. Therefore it is vital that staff at South Tees Hospitals NHS Foundation Trust adhere to the policies and procedures that have been developed to ensure that adequate safeguards are in place for the processing of personal data.

3.4 <u>Information Governance Assurance Statement of Compliance (SoC)</u>

3.4.1 The Information Governance Assurance Statement of Compliance (SoC) is the agreement between NHS Connecting for Health (CfH) and Approved Service Recipients. It sets out the information governance policy and terms and conditions for use of NHS Connecting for Health services.

3.4.2 The SoC contains a number of obligations to enable use of NHS CfH’s services, which aim to preserve the integrity of these services. It is essential that every organisation meets its Statement obligations to the required standards to safeguard NHS CfH’s services and information for all. The Trust currently uses a number of these services such as the Choose and Book system for appointments and referrals, and the Summary Care Record for the validation of patient demographics.

3.4.3 To achieve SoC the organisation has to achieve Level 2 or above on the requirements of the IG Toolkit. Where the minimum IG Toolkit standards are not met an action plan for making the necessary improvements must be agreed with the Department of Health Information Governance Policy Team (currently via the strategic Health Authority).

The Trust declared itself SoC compliant in 2011/12 as although the Trust had two standards scoring below the required minimum level 2, action plans were in place for these requirements and were submitted to the SHA for approval.

3.5 <u>Monitor</u>

3.5.1 Monitor’s Compliance Framework for 2011/12 confirms that:

- NHS Foundation Trusts were required to achieve a minimum of level 2 performance against the requirements of their IG Statement of Compliance (SoC) in the IG Toolkit.
- Any key risks to compliance with the Trust’s Authorisation must be identified and addressed.
- A failure to ensure information governance procedures are in place and operating may be reflected in the governance risk ratings.

The Trust has declared itself SoC compliant albeit with action plans in place to achieve compliance on 2 standards scoring below level 2.

3.6 Policies

3.6.1 There has been a lot of scrutiny, government reports and recommendations recently around information governance, in particular around data handling. To ensure that the Trust's policies reflect the new guidance a review has been carried out, and a new structure has now been identified incorporating an "Information Governance" section on the Trust's intranet site for staff to easily identify the relevant individual policies and guidance.

3.6.2 An IG policy plan is in place for the on-going management of current and newly identified policies and Standard Operating Procedures (SOPs) ensuring alignment with community services where required.

3.7 Information Governance Board Assurance

3.7.1 In November 2011 a report was received by the Integrated Governance Committee setting out the Trust's position with regards to current practices to deliver information governance as outlined in the Guidance for NHS Boards: Information Governance (Aug 2011) as well as the joint letter from the Department of Health (DH) and the Information Commissioner's Office (ICO) (September 2011). The report set out the key areas to which Boards must assure themselves, supported by organisational statements which confirmed robust practices across the information governance agenda.

4. Information Governance Progress 2011/12

4.1 Audit & Monitoring – Information Governance Toolkit Assessment & Results

4.1.1. NHS organisations are mandated to submit, via Connecting for Health, an annual self-assessment of their information governance status. This is achieved via the Information Governance Toolkit (IG Toolkit). The IG Toolkit is used to measure progress against key requirements. The 2011/12 IG Toolkit scores were required to be submitted thrice yearly:

- 31 July 2011 - Benchmark submission
- 31 October 2011 - Baseline submission
- 31 March 2012 - Final submission

4.1.2 The IG Toolkit uses a framework of standards, which are designed to ensure organisational compliance with statutory and mandatory requirements concerning the management of patient, staff and corporate information. The IG Toolkit has been developed as the principal mechanism by which IG policy can be broken down into measurable components in order to assess an organisation's performance annually through a system of self-assessment and audit. The IG Toolkit enables the organisation to develop a strategy and annual work programme to raise the level of compliance year-on-year, and also improve its information risk management process.

4.1.3 The IG Toolkit assessment score is used to inform the National Information Governance Board and the Care Quality Commission. NHS Quality Accounts now include IG assurance within their performance assessments. A requirement for internal audit of IG has been formally established by including IG performance in NHS organisations' statement of Internal Control and Annual Report.

4.1.4 The Information Governance Toolkit currently encompasses the following:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information assurance

- Secondary Use Assurance
- Corporate Information Assurance

4.1.5 Connecting for Health review the requirements of the Information Governance Toolkit annually to ensure the following functional aspects:

- to provide interpretive advice and guidance
- to provide a means of self assessing performance against key aspects of information governance
- to support the independent assurance of information governance returns

4.1.6 The IG Toolkit End of Year Report 2011/12 was submitted as a position statement of 75% to the Integrated Governance Committee at it's meeting on the 14th March 2012. The final score was confirmed at 73% and was submitted by the Trust at the end of March 2012 and included community services as part of the overall Trust's submission. The scores provided by the Trust are required to be internally and externally verified by:

- Internally - The Trust's Head of Financial Governance and Control prior to final submission.
- Externally – The Trusts Internal Auditors, Audit North provide a sample review of standards within the Toolkit prior to final submission. The auditors produced a report which concluded in significant assurance with no recommendations.

4.1.7 All standards, apart from standard 112 and 324 were scored a minimum of a level 2 prior to 31st March 2011. Table 1 provided the Trust with a position statement prior to the final submission, and highlighted requirement 112 with a possibility of a level 3 still being achievable, however by the end of March training compliance had dropped to 70% and scored a level 1. As the Trust's expected MIS system was put on hold a Standard Operating Procedure was discussed to help achieve level 2 compliance for standard 324 Pseudonymisation, however this was not possible due to the shortened timeframe and amount of work required to achieve this standard.

4.1.8 Action plans were in place for the undermentioned and monitored by the IGSG to ensure that the Trust could provide assurance to Connecting for Health and Monitor if requested. Table 2 compares acute trusts across the Strategic Health Authority.

Table 1

Req No.	Requirement Definition	Score Oct 2011	Position Statement	Predicted Score March 12	
112	To ensure organisational compliance with the law and central guidelines relating to Information Governance (IG), staff must receive appropriate training. Therefore, IG training is mandatory for all staff, (comparable to health and safety training) and staff IG training needs should be routinely assessed, monitored and adequately provided for.		All staff (95%) must complete mandatory IG training on an annual basis. This standard also requires an IG training programme based on a training needs analysis for all staff and additional training for key staff groups. Currently (upto 14th February) 61% of staff are compliant, having refreshed their training within the last 12 months. The Trust is experiencing a reduction in compliance month on month due to last years push to ensure all staff undertook the training (eg Dec 2011= 74% compliant, February 2012 = 61% compliant). Awareness of this has been raised with senior staff as well as divisional IG representatives and training links to ensure staff check when their training is due in order to maintain/raise the percentage compliance.	**1**	**3**

Req No.	Requirement Definition	Score Oct 2011	Position Statement	Predicted Score March 12
			Reports have been sent to Divisional Managers and Corporate Directors highlighting those staff whose training has or is about to expire prior to 31st March. Communication has been constant across the Trust by various methods in order to raise awareness of staff compliance by 31st March 2012 and supported corporately. An additional programme of delivered sessions as well as divisional ad-hoc sessions has also been available to staff over the last 12 months to help widen the options for staff compliance. Delivering, monitoring and reporting on the IG training element has become a major drain on IG resources. A bid for 12 months support through the Trust's corporate mandatory training budget has been successful and will help to establish and embed a focused IG training analysis and access route for all staff groups.	🟥 🟩
324	A fundamental principle of the Data Protection Act 1998 is to use the minimum personal data to satisfy a purpose and to strip out information relating to a data subject that is not necessary for the particular processing being undertaken. This principle is aligned with the Caldicott Principles familiar to NHS and Social Care organisations and is supported by both common law confidentiality obligations and the Human Rights Act 1998 which provides a privacy right for individuals.	🟥 **1**	The Trust decision to establish a Management Information System which will incorporate the process change along with the functionality required to pseudonymise person identifiable data for secondary use purposes, is currently on hold. Due to the above the Head of Information is working closely with the IG Department to identify alternative process change along with suitable tools required, to establish an internal Safe Haven for information exchange and pseudonymisation functionality for secondary use purposes. An action plan is in place and a draft Standard Operating Procedure for the Secondary Use of Data has been developed and under consultation, however, in order to reach Level 2 compliance the internal processes, tools and any action/project plan must be complete and signed off by the organisation. Every effort is being made to achieve this standard as soon as practically possible, however due to the impact on internal process and systems this standard may not be achieved by March 2012.	🟥 **1**

Table 2

PUBLISHED TOOLKIT SCORES 31st MARCH 2012 (VERSION 9)	%	RAG
SOUTH TYNESIDE FOUNDATION NHS TRUST	75	Satisfactory
CITY HOSPITALS SUNDERLAND NHS FOUNDATION TRUST	83	Satisfactory
GATESHEAD HEALTH NHS FOUNDATION TRUST	81	Satisfactory
THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST	71	Satisfactory
NORTHUMBRIA HEALTHCARE NHS FOUNDATION TRUST	88	Satisfactory
SOUTH TEES HOSPITALS NHS TRUST	73	Not Satisfactory
NORTH TEES AND HARTLEPOOL NHS FOUNDATION TRUST	80	Not Satisfactory
COUNTY DURHAM AND DARLINGTON NHS FOUNDATION TRUST	71	Satisfactory

4.1.9 The IG Toolkit levels of scoring are based on a two tier Red (unsatisfactory) or Green (satisfactory) system of reporting. Connecting for Health have classified that having one standard “red unsatisfactory” will impact on the overall status of the toolkit as “red unsatisfactory”, thus giving a false reflection of an organisations overall general IG performance. As such, although the Trust is scoring red on 2 standards, the overall compliance of the Trust was 73% against the revised toolkit.

4.1.10 All responsible requirement owners’ collated electronic evidence in the secure section of the allusers fileshare and a work programme was kept up to date by the Information Governance team. Information Governance staff undertook training on the use of Health Assure and this facility is now planned to be utilised upon the release of v10 of the IG Toolkit. A work program for each requirement was monitored by the Information Governance Steering Group (IGSG) on a bi- monthly basis.

4.1.11 Table 3 highlights the separate GP IG Toolkit score for the Marske Medical Centre and the Resolution Centre. These are highlighted as discussions will be had around the possibility of a single inclusive IG toolkit for submission which will reflect the organisation as a whole for 2012/13

Table 3

GP IG Toolkit v9 Completion	Overall Score	Grade
Marske Medical Centre	79%	Satisfactory
Resolution Centre	79%	Satisfactory

4.2 Confidentiality and Data Protection Assurance

This area of work specifically addresses**:**

- NHS Code of Practice: Confidentiality
- Data Protection Act 1998

4.2.1 Incident Management

4.2.1.1 The Trust must publish details of any personal information related incidents categorised as Serious Untoward Incidents (level 3-5) as part of the Statement of Internal Control and Annual Report. Between April 2011 and March 2012, there were no serious untoward incidents of the severity rating 3-5. Personal data related incidents classified at a severity rating of levels 1 and 2 are summarised in the required Department of Health format in table 4 below.

Table 4

Summary of Personal Data Related Incidents In 2011/12 LEVEL 1-2 ONLY		
Category	**Nature of Incident**	**Total**
I	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	0
II	Loss of inadequately protected equipment, devices or paper documents from outside NHS premises	0
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	0
IV	Unauthorised disclosure	5
V	Other	0

4.2.1.2 In all of the incidents of unauthorised disclosure above the Trust had no evidence that any confidential personal information had been seen by anyone outside of the Trust's employment.

4.2.1.3 The Trust has shown a steady decline over the past 3 years in the number of Serious Untoward IG incidents as evidenced in the Trust's Annual Reports

Table 5

Category	Nature of Incident	09-10	10-11	11-12
I	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	8	2	0
II	Loss of inadequately protected equipment, devices or paper documents from outside NHS premises	0	0	0
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	1	0	0
IV	Unauthorised disclosure	0	0	5
V	Other	0	4	0
Total		**9**	**6**	**5**

4.2.1.4 However the number of potential breaches of confidentiality reported on the Datix system shows a steady increase over the same time period. This is almost certainly due to the heightened awareness of the importance of Information Governance throughout the Trust which has been accomplished through a steady programme of staff awareness and briefings though the Staff Bulletin and the IG EYE quarterly newsletter as well as numerous sessions of delivered IG training and increasing numbers of staff undertaking the on-line IG e-learning programme.

Table 6

	2009-10	2010-11	2011-12
Potential breaches reported on Datix	**88**	**123**	**153**

4.2.1.5 A Clinic Notes in Transit Report was completed in November 2011 which detailed the nature of a near-miss incident that had occurred. A number of options were presented for improving the security of the process as part of the lessons learned. The process is currently being evaluated by the Health Records Manager and the Pathology department to find the most appropriate and cost effective means of transferring patient-identifiable data across hospital sites.

4.2.2 Standardisation of Data Protection Processes

4.2.2.1 Under the Data Protection Act (DPA) 1998 organisations have a statutory duty to respond to requests for personal information within a time period of 40 calendar days. However although DPA states 40 days to comply, a Government commitment requires that for health records, requests should normally be handled within 21 days.

4.2.2.2 The review of the Trusts Data protection processes for the handling of subject access requests is still on-going and meetings have taken place to discuss a single point of contact and standardised reporting system across the organisations for all such requests.

4.2.2.3 Table 6 illustrates the total number of requests received by South Tees Hospitals NHS Foundation Trust for 2011-2012.

Table 6

	Ad Hoc Data Protection requests	Requests via Legal services	Access to Health Care Records	Total
April	2	10	267	279
May	1	11	214	226
June	3	10	244	257
July	2	12	258	272
Aug	0	10	231	241
Sept	0	5	197	202
Oct	4	5	254	263
Nov	3	7	216	226
Dec	1	8	194	203
Jan	1	14	254	269
Feb	4	13	286	303
Mar	0	8	225	233
Annual Totals	**21**	**113**	**2840**	**2974**

4.2.3 Information Sharing

4.2.3.1 The Trust worked in co-operation with Teesside Hospice to review and update the current information sharing agreement. Work is underway with the Butterwick Hospice to implement a similar information sharing agreement to the above.

4.3 Information Security & Information Risk Management Assurance

4.3.1 Information Security

4.3.1.1 The Information Governance team has supported and encouraged the use of the national Information Governance Training Tool provided by Connecting for Health. This has proven to be extremely useful in providing training and guidance to all levels of staff across the Trust. It utilises information security guidance videos and slides to provide advice and knowledge appropriate to staff roles.

4.3.1.2 The Trust's Deputy Information Governance Manager oversees a fortnightly Formal Trust IT Security Meeting attended by the ICT Communications Manager & the ICT Infrastructure Security Analyst (Advanced). This group ensures that the Trust can constantly review emerging threats and issues and provides expert guidance and action in relation to the Information Security agenda. Any actions are minuted to ensure compliance with issues are monitored and evidence is available for review by Audit.

4.3.1.3 A number of Information Security reviews have been performed over the course of the year, the most significant being:

- Secure disposal of media - Greenworld
- Confidential waste – PHS
- Digital Dictation – Bighand
- Paediatric Diabetes System – Twinkle.net
- Transfers of Patient Identifiable Data outside of the EEA :
    - Merlin.net
    - Stryker Knee

4.3.1.4 All Information Security Reviews have followed the Trust Information Risk Management Framework procedure of being provided to the SIRO for review and approval and where appropriate an accompanying Caldicott Approval Form has been completed by the external company and approved by the Trust Caldicott Guardian.

4.3.1.6 The Trust's Deputy Information Governance Manager chairs the NESHA IG Security Sub-Group. This group meet quarterly to discuss various national/local issues and advises health and social care organisations across the SHA on Information security concerns.

4.3.1.7 A Forensic Readiness SOP has been produced and implemented within the Trust utilising best practice guidelines from the Police and also guidance provided by the Trusts Internal Audit providers – Audit North. This document helps to assure the Trust that in the event of an Information Security incident, appropriate protocol is followed in strict sequence, thereby preserving the chain of evidence if the incident becomes a police matter.

4.3.1.8 Due to the current rising trend of utilising off-site storage services and cloud based activities, the Deputy Information Governance Manager has attended a two day training course on Cloud Computing Security Knowledge which highlighted a number of serious concerns relating to the use of such services, within an NHS environment, in which IG Security measures must be considered and applied.

4.3.2 <u>Information Risk Management</u>

4.3.2.1 The Digital Information Policy Unit within Connecting for Health, issued the guidance document "NHS Information Risk Management" (January 2009). It reflects Government guidelines and is consistent with the Cabinet Office report on "Data Handling Procedures within Government".

4.3.2.2 The key requirement is for information risk to be managed in a robust way within work areas and not to be seen as something that is the sole responsibility of IT or IG staff. It is important that this is consistent across the Trust and to achieve this, a structured approach was implemented, building upon the existing information governance framework within which many parts of the NHS are already working.

4.3.2.3 The Trust adopted and implemented the national framework using a structured approach. The Trust assigned the "ownership" of information assets to senior accountable staff. Divisional Managers and Corporate Directors were appointed Information Asset Owners (IAO's) and operational staff, with day to day responsibility for managing risks to their information assets, appointed Information Asset Administrators (IAA).

4.3.2.4 Information Governance staff met with each IAO to discuss the Information Risk Management Framework and IAO responsibilities. A number of Information Risk Management presentations have taken place within divisions/directorates to provide more detail and awareness on the role of IAO's and IAA's.

4.3.2.5 An Information Risk Management Framework pack was developed to ensure the successful integration of IRM across the Trust and required each IAO to confirm compliance with a number of risk management standards within the Information Governance Toolkit or complete an appropriate action plan.

4.3.2.6 An internal audit was performed within the area of Information Risk Management during 2011/12 and identified a number of recommendations. The IG department are currently supporting IAO's and IAA's in order to achieve compliance with the recommendations. For example the Trust needed to ensure that the framework was fully embedded within its organisational structure and that all IAO's and IAA's are required to have completed the appropriate e-learning for their role with regards to Information Risk Management. A review of the training provided was performed by the IG department and it was established that although one to one training had been provided to all IAO's the Policy document required staff to complete the online training module within the Information Governance Training Tool. This action has now been completed.

4.3.3 E-Safety – Safeguarding in a Digital World

4.3.3.1 The Local Safeguarding Children Board (LSCB) has an expectation that the Trust develops an environment where children, young people and adults who work with them can use the Internet and other digital technologies safely and securely.

4.3.3.2 South Tees NHS Foundation Trust takes seriously the role it has to ensure that it co-operates to safeguard and promote the welfare of children and young people in the locality, and to ensure that the Trust is effective in doing so. The Head of Information Governance is currently the Trust E-safety Lead and is working in partnership with the Safeguarding Team to ensure that awareness training forms part of the Trusts Safeguarding Children training. This ensures that staff are aware of their responsibilities to e-safety and safeguarding children in a digital world.

4.3.3.3 As part of promoting the welfare of children and young people in accordance with the Children Act 2004 and Working together to safeguard children 2006, the LSCB has devised an e-safety strategy plus a policy that is built on four key areas:

1. Policies, practices and procedures
2. Education and training
3. Infrastructure and technology
4. Standards and inspection.

4.3.3.4 The Trust currently has an E-safety Action Plan in place, monitored by the Information Governance Steering Group. This action plan will contribute to the LSCB Section 11 compliance audits (M*ulti-agency safeguarding children information to assist good practice*).

4.4 Corporate Information Assurance

This area of work specifically addresses**:**

- Freedom of Information Act 2000
- NHS Code of Practice: Records Management

4.4.1 Freedom of Information

4.4.1.1 The Freedom of Information Act (FoIA) came into force at the beginning of 2005. It deals with access to official information, while parallel regulations deal with environmental information. The Act provides individuals or organisations with the right to request information held by a public authority. They can do this by letter or email. The public authority must tell the applicant whether it holds the information and if so, must supply it within 20 working days, in the format requested (unless exemptions apply). The Act is fully retrospective and applies to all information, not just information filed since the Act came into force. Compliance with the Act is overseen by the Information Commissioner's Office which is the UK's independent authority set up to promote access to official information and to protect personal information.

4.4.1.2 The Freedom of Information Policy has been revised to standardise the processing of requests across all the Trust including Community Services. The Policy now includes information on accessing information using the Environmental Information Regulations and so has been re-named the Public Access to Information Policy. There are 3 associated Standard Operating Procedures which are:

SOP 10 - Procedure for processing requests for information under the Freedom of Information Act 2000

SOP 11 - Procedure for processing requests for information under the Environmental Information Regulations 2004 (EIR)

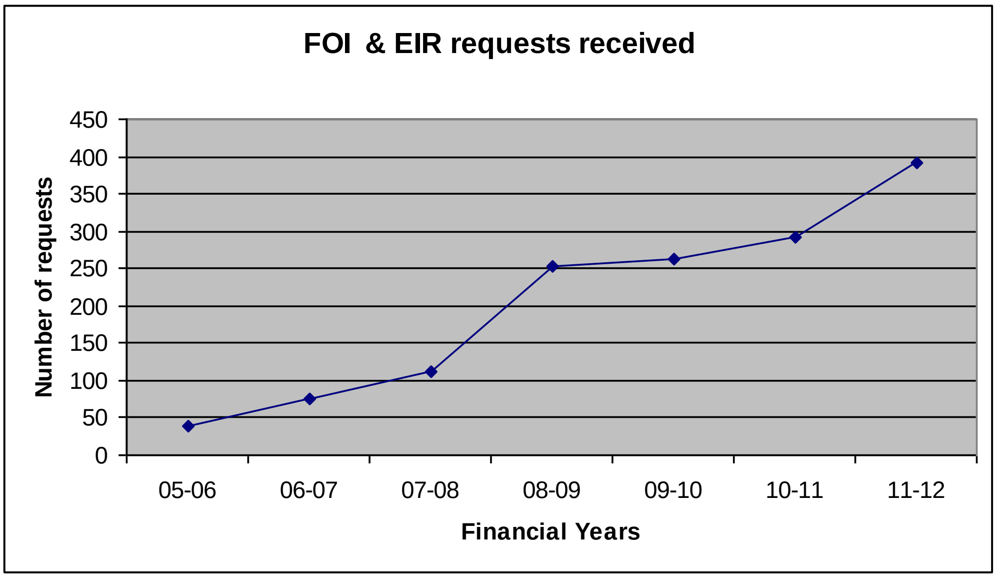
SOP 12 - Requests for information under FOI and EIR - internal review procedure

4.4.1.3 A procedure has been written to aid the identification and handling of suspected multi-organisational 'round robin' FoIA requests which will assist in giving advanced notice of any media interest as well as ensuring a consistent response to such requests across the region as a whole.

4.4.1.4 All responses to a FOIA or EIR request now include a customer satisfaction survey. Out of all the requests received in the last financial year only 15 surveys were returned. However the responses received were very encouraging.

	Very Good	Good	Satisfactory	Poor
Quality of service provided	11	4		
Timely acknowledgement of request	11	3	1	
The degree to which the response answered your request	10	3	2	
Ease of understanding of the response	13	2		
Overall helpfulness of the response	10	5		

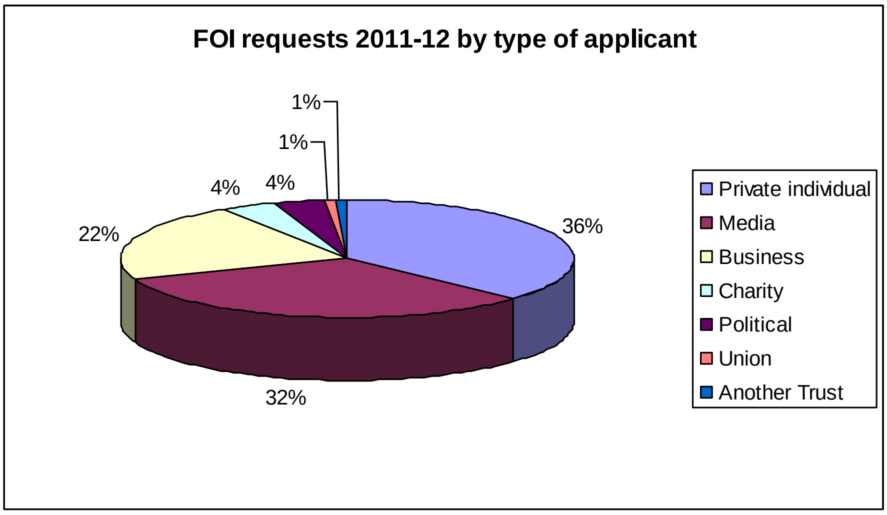
4.4.1.5 The Trust has received 392 FOI requests for the year 2011-2012; this represents a 34% increase on last year and shows a continued year on year rise in the number of requests received. This continued increase in both the number and complexity of requests poses a significant burden on Directorates and Divisions.



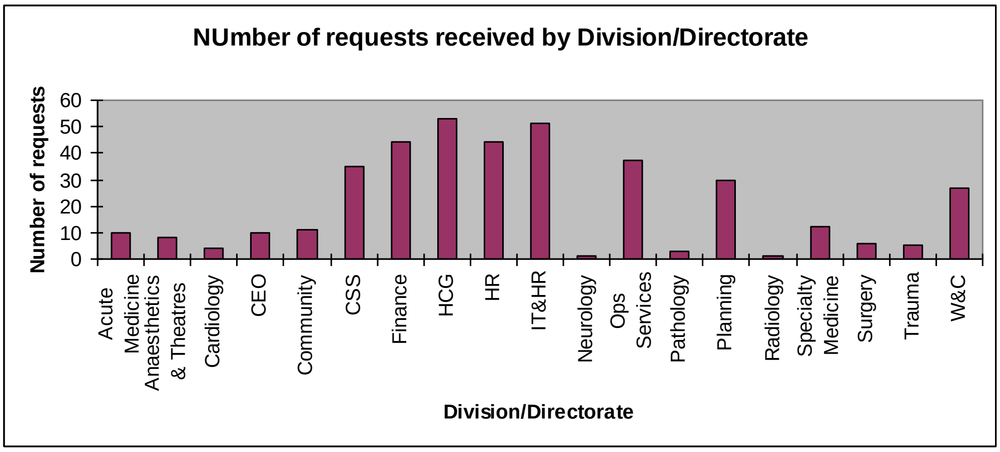
4.4.1.6 There has been a significant increase in the number of requests where an exemption under FOIA is applicable. For Q1 2011-12 an exemption was used in 5% of the requests received, whereas for Q1 2012-13 an exemption was used in 17% of the requests received. The use of exemptions reduces the work required of Divisions and Directorates as they do not have to locate and supply the requested data. In contrast however, the use of an exemption imposes an extra burden on the Information Governance input to FOI requests as the compilation of the legal arguments necessary to ensure the response meets the expected ICO standard takes a significant amount of time to assemble.

4.4.1.7 Unfortunately the Trust continues to have issues with achieving the 20 day time limit for responses and over the year 19% of responses have gone over that statutory limit. One of the reasons for this may be that requests are now much more complex than they were 2 or 3 years ago and often involve input from several departments. In some instances one department cannot process their part of a request until data is provided by another department first. In order to address this problem, update training was offered to all Personal Assistants to Directors and Divisional Managers to remind them of the importance of processing requests as speedily as possible,

4.4.1.8 The table below shows the percentage requests by applicant type. Requests from private individuals have increased from 29% last year to 36% this year. However this statistic should be viewed with caution as applicants often use personal email addresses to try to disguise requests that are submitted for a work purpose (either media or business) and so are recorded as being from a Private individual by default.



4.4.1.9The table below shows the number of Freedom of Information requests received by each Division/Directorate in 2011-12.



4.4.1.10 Every public authority, subject to FoIA, must adopt and maintain a publication scheme. A publication scheme is a commitment to routinely and proactively provide information to the public. The model publication scheme, as detailed in the Definition Document for Health Bodies (October 2008), was adopted by the Trust in January 2009 and is available to the public via the Trust internet site. In 2011 The Information Commissioner's Office promised to issue renewed guidance regarding what needs to be included in a Publication Scheme and this is still awaited. In the meantime the Trust's Internet site will be based on the 2008 model publication scheme. The responsibility for updating the information within the publication scheme lies with the divisions/directorates whose information it is.

Since 2005 and the introduction of FoIA all FOI requests have been logged on the Datix system. Before amalgamation with the Trust, MRCCS used the MIDAS system to log their FOI requests. During the coming year the IG team will conduct an evaluation of both systems to see which system provides optimum benefit for recording requests and producing reports.

4.4.2 Records Management

4.4.2.1The Records Management Policy has been updated to incorporate the Community Services Division and associated Standard Operating procedures have also been developed. They are as follows:

SOP01 -	Procedure for the creation of corporate records
SOP02 -	Procedure for the Storage and Disposal of Records – All Divisions/Directorates except Community Services
SOP 03 -	Procedure for the Storage and Disposal of Records - Community Services Division (formerly MRCCS)
SOP04 -	File retention and archiving of data created from live information systems
SOP05 -	Appraisal and disposal of records
SOP06 -	Procedure for scanning records

4.4.2.2 All requirements relating to corporate records management within the IG Toolkit for the year 2011/12 reached the required level 2 compliance.

4.4.2.3 It is disappointing that there has been little progress with Divisions and Directorates completing the Information Asset Register via the web-based tool. This tool has been in place for 3 years now and despite numerous meetings with representatives from various work areas very little progress has been made. However, recognition should be given to the Healthcare Governance Directorate for the organised way they approached this task which allowed them to complete their input to the web-based tool swiftly and requiring only 44 entries to cover the record sets relating to all the diverse responsibilities of that Directorate.

4.4.2.4 The IG team will conduct an evaluation of the Trust's web-based tool against the MIDAS system which was used by the Community Services Division when they were MRCCS. The MIDAS system contains a section for the registration of information assets including hardware, software and record sets and may provide an opportunity for compilation of a comprehensive Trustwide Information Asset Register.

4.5 Connecting for Health (CfH) & the National Programme for IT (NPfIT)

4.5.1 Registration Authority (RA)

4.5.1.1 The NHS Care Records Service Registration Authority is responsible for registering and verifying the identity of NHS staff that need to use the NHS Care Records Service and related IT systems and services, including Choose and Book and the Electronic Staff Record.

4.5.1.2 Access to these computer systems and services is controlled by smartcards with photographic ID and pass code, similar to a chip and pin credit card. Registration authorities issue smartcards to staff which hold appropriate levels of access to systems and subsequent patient information after an e-GIF level 3 identity check has been completed and organisational sponsorship provided. This is essential to protect the security and confidentiality of every patient's personal and healthcare information.

4.5.1.3 A project team has successfully implemented the first stage of Integrated Identity Management which is a national requirement to integrate HR with RA and eliminate duplication of identity checks. The project team initially endorsed the idea of a *one-stop-shop* to be located in the main hospital designed to provide existing and new employees with a central location to obtain/maintain their ID badge, Smartcard, parking permit etc. To achieve this, it was acknowledged that recruitment / payroll processes would need to be streamlined with RA processes. These are now under review to ensure a smooth transition to Integrated Identity Management.

4.5.1.4 The management of Smartcard maintenance, including unlocking and renewing, has been delegated across the organisation. This includes the set-up of RA Workstations across divisions/locations to ensure staff are able to easily amend their Smartcard when necessary. The RA Manager will audit all activity on any workstations that are set up to ensure consistency and secure smartcard management is upheld across the organisation.

4.5.1.5 The RA function for community services is currently managed via a service level agreement with Middlesbrough PCT and North Yorkshire & Yorks PCT until further notice.

4.5.2 Integrated Identity Management

4.5.2.1 It is important that everyone who will have access to patient information has been through the same rigorous identity checks. Integrated Identity Management allows these checks to be done once, at the stage of employment, rather than repeated a second / third time during employment. The integration of the RA system (UIM) and the Payroll system (ESR) means that the level of access to patient information an individual will have, will be decided by their position in the organisation.

4.5.2.2 The Integrated Identity Management communication from CfH is encouraging organisations to look at three key areas: HR / RA integration, Position Based Access Control (PBAC) and the Smartcard/ESR interface. The trust is now live with the Smartcard/ ESR interface and the RA Manager and Payroll team have so far successfully allocated over half of all Smartcard users with a specifically allocated PBAC agreed by the organisation. This control ensures that levels of access are determined by ESR position meaning that no one member of staff has more or less access than they require to carry out their job role. Recruitment staff are now logging ID checks into ESR meaning that duplication of ID checking for elements such as Smartcards has been removed. The RA project team are working together to achieve Integrated Identity Management within South Tees which will ensure robust identity checking procedures and a higher level of control over access to NHS CRS and also guarantees a streamlined recruitment process within which there will be no duplication of identity checking.

4.5.3 Summary Care Record Implementation into Secondary Care

4.5.3.1 The Summary Care Record application (SCRa) is currently used amongst clerical staff to obtain patient demographics, NHS numbers and GP details. The full Summary Care Record (SCR) allows Clinicians to access information such as any medication the patient is on / has been on and any allergies or adverse reactions the patient has. Both levels are accessed through the secure National Spine Portal using minimum search criteria of gender, surname and date of birth. As with other National Spine applications, access is controlled by a combination of smartcard privileges (Position Based Access Control or 'PBAC') and system control based on "legitimate relationships" with patients.

4.5.3.2 South Tees was the first acute Trust in the North East to introduce the SCR into secondary care and worked collaboratively with Connecting for Health to produce a Business Change and Information Governance Model for Viewing Summary Care Records and a staff SCR e-learning module, for use by other Trust's nationally.

4.5.3.3 Initially the Summary Care Record (SCR) was used in the following areas, A&E, AAU Ward 1 (Male), AAU Ward 15 (Female), Ward 28 Elderly Care and pharmacy staff. The uptake and usage was very good in the AAU wards and with Pharmacists and work is underway to increase the usage within A&E and Elderly care areas. The Trust is supporting the PCT to increase the upload of SCRs by GPs as the current upload stands at around 60%. Regular reports of usage are delivered to the SCR project team.

4.5.4 SystmOne Unit Transfer

4.5.4.1 A report was written in October 2011 to highlight the pending requirement to transfer selected SystmOne Units from the PCTs to South Tees as a result of the Transfer of Community Services. The paper highlighted the risks involved and provided options as to a way forward with the process. The RA Manager has since worked closely with the PCT staff and relayed relevant information about the transfer of the SystmOne units back into South Tees. Workgroups under South Tees have been created, which mirror what is currently set up in the PCT so that the transfer can take place.

4.5.4.2 In the upcoming months, the selected Community units will be transferred from the PCTs to South Tees under our newly obtained South Tees SystmOne reporting unit.

4.6 IG Training Needs & Awareness

4.6.1 In line with recommendations in the Information Governance Assurance Programme and the NHS Operating Framework, information governance training became mandated for annual completion by staff. A key driver in support of this was the IG toolkit requirement for training, in which the Trust was required to evidence that 95% of its workforce had completed the mandatory Information Governance training module by 31 March 2012.

4.6.2 Mandatory training compliance is monitored by Human Resources; and confirmed only 70% compliance at the end of March 2012. The Trust experienced a reduction in compliance month on month due to the previous years push to ensure all staff undertook the training (eg Dec 2011= 74% compliant, February 2012 = 61% compliant). Awareness of this had been raised with senior staff as well as divisional IG representatives and training links to ensure staff checked when their training was due in order to maintain/raise the percentage compliance. Reports were sent to Divisional Managers and Corporate Directors highlighting those staff whose training had or was about to expire prior to 31st March.

4.6.3 The information governance team efforts in delivering, promoting, administering and monitoring the training had proved a drain on resources, seeing 4 staff each delivering up to six training sessions per day in the run up to March 2012. A bid for 12 months support through the Trust's corporate mandatory training budget has been successful and will help to establish and embed a focused IG training analysis and access route for all staff groups. Monitoring training especially with the Community Services division has proved very difficult due to the localities and number of different systems used in order to record staff training

4.6.4 The IG department felt an increase in IG queries particularly relating to community services operational issues and processes presumed highlighted by mandatory training and awareness briefings.

4.6.4 Information governance also forms part of the Trust's Risk Assessment Training Programme. This training gives awareness and guidance on how to conduct an Information Risk assessment as well as reporting and investigation of information incidents.

5. Information Governance Key Drivers and Work Plans for 2012/13

A high level Information Governance Action Plan has been developed (see Appendix B) which encompasses the Trusts priorities and key milestones within the current IG Framework. A number of detailed actions plans are in place to support the high level plan.

5.1 Audit & Monitoring – IG Toolkit

5.1.1 The IG Toolkit v10 was released in June 2012 and is currently under review by the IG team to assess any changes in the requirements which may have an impact on establishing a new baseline for the Trust.

The Trust is required to report three times in year as follows:

- 31st July 2012 - Baseline assessment
- 31st October 2012 - Progress Update
- 31st March 2013 - Final submission

5.1.2 Appendix C highlights the IG toolkit v10 requirements and proposed baseline scores for 2012/13. Due to the tight timescale for submission the baseline score is based on the requirement scores submitted in March 2012. A review of all requirement compliance will take place across the Trust in preparation for the Progress Update in October 2012, allowing an improved understanding of IG compliance.

5.1.3 2012/13 will see the v10 IG Toolkit Work Programme integrated into the Trusts Health Assure system, and updated regularly to evidence measures of achievement.

5.1.4 Standard 112 – IG Training is currently not meeting the minimum level 2 requirement and as such has an action plan in place that will be monitored by the IG Steering Group on a bi-monthly basis (see 5.7 for further information).

5.1.5 Standard 324 – Pseudonymisation is currently not meeting the minimum level 2 requirement. An action plan will be monitored by the IG Steering group on a bi-monthly basis (see 5.5.12 for further information).

5.1.6 The Information Governance Steering Group will monitor the High Level Action Plan and the IG Toolkit Work Programme, the minutes of which will be received into the Formal Management Group. The proposed IG Toolkit submission scores will be presented to the Integrated Governance Committee to provide assurances that the Trust is achieving the required level of compliance with legislation and national standards.

5.1.7 The Information Risk Management framework relies heavily upon the requirements of the IG Toolkit; once v10 requirements have been reviewed, further guidance and/or actions to ensure compliance will be disseminated via the Trust's IRM structure. Any outstanding recommendations from the 2011/12 IRM audit will also be included in any workplans.

5.1.8 Internal audit will review the Trust's compliance against the IG Toolkit. A number of related audits are also scheduled for 2012/13 such as PC and Data Management and use of mobile devices within community.

5.1.9 As discussed at 4.1.11 further dialogue around the separate submission of the 2 GP practice toolkits are underway. It is likely that the July benchmark for the practices (based on March 2012 submission) will be submitted by 31st March whilst awaiting any amalgamation requirements which will then hopefully see 1 IG toolkit submission in 2012/13 for South Tees as a whole.

5.1.10 From June 2012 the IG department are pleased to welcome Henrietta Wallace as the "IG Champion". As a Non-Executive Director of the Board Henrietta will promote and support good information governance across South Tees Hospitals NHS Foundation Trust.

5.2 Legislation, National Standards & Policy

5.2.1 The NHS Operating Framework for 2012/13 stresses that the protection of sensitive patient information remains a top priority for the NHS and that Data loss is not acceptable where adherence to agreed national policies would have prevented the breach. The framework requires organisations to be vigilant at all times and to ensure that appropriate governance policies and guidelines are implemented and followed in practice.

5.2.2 The Information Governance department/Toolkit v10 requirements will feed into the following governance arrangements where required:

- Care Quality Commission (CQC).
- NHS Quality Accounts.
- Statement of Internal Control.
- Trust Annual Plan.
- Trust Annual Report.

5.2.3 An IG Policy Plan is in place to continue the review/development of policies. The plan incorporates the current gap analysis with community services to ensure robust and consistent policies across the integrated organisation as a whole.

5.2.4 A review of the Trust's Overarching IG Policy will take place to ensure an appropriate and robust information governance framework across the Trust.

5.3 Confidentiality & Data Protection Assurance

5.3.1 Regional concerns around IG incident reporting have been escalated nationally and subsequently a review of incident management is underway. This may have a significant impact on the way in which IG incidents are graded and escalated to the appropriate authorities. There are currently national discussions supporting the IG Toolkit as the vehicle for reporting IG serious untoward incidents instead of the current STEIS system. The impact of these changes are currently unknown.

5.3.2 As seen in 4.2.1.4 the number of potential breaches of confidentiality reported via the Datix system has shown a steady increase. The IG team will continue to raise awareness of such incidents via the Trust STARS system (Risk Alerts/Updates) and all-user briefings where necessary, to help mitigate the risk of similar incidents being repeated. The IG department will also review the ICO Monetary Penalty Notices to ensure that any lessons learned from these incidents can be shared and acted upon within the Trust where necessary.

5.3.3 The Information Governance Department are currently progressing the standardisation of data protection and subject access request processes across the organisation to ensure consistency in compliance with the Act. Currently a number of systems are used across the Trust to administer requests for information. Community services staff currently use a central system to record requests (MIDAS), An evaluation of these systems will be undertaken to ensure a centralised system that is fit for purpose and is available across all hospital and community services sites.

5.3.4 IG will carry out spot checks in departments to provide evidence that staff are compliant with Data Protection & confidentiality. The need to evidence service user satisfaction with regards to confidentiality will be undertaken via patient satisfaction surveys lead by Healthcare Governance.

5.3.5 Due to successful funding for an IG trainer work is already underway with divisions and directorates to ensure that all staff (Minimum 95%) comply with the annual mandatory IG training requirement. A training plan is in place and is monitored on a bi-monthly basis by the IG Steering Group for assurance.

5.3.6 The IG department will review, develop and monitor Trustwide information sharing protocols including policy and guidance for staff.

5.4 Corporate Information Assurance

5.4.1 Freedom of Information Act 2000 (FoIA)

5.4.1.1The IG department will review, evaluate and improve the Trust corporate system for the handling and monitoring of FoIA requests to ensure compliance with the statutory 20 day time frame.

5.4.1.2 The IG department will offer training / update sessions on FoIA as well as the handling of requests and an approach to pro-active publication of divisional/directorate data to ensure statutory compliance.

5.4.2 Records Management

5.4.2.1 The Records Management Strategy, supported by Policy and associated standard operating procedures, will be reviewed and escalated across the Trust.

5.4.2.2 IG will work with divisional IG representatives to support the identification and registration of divisional Information Assets.

5.4.3 The Protection of Freedoms Act 2012

5.4.3.1 The above Act was given royal assent on the 1st May 2012 but as yet no date for enforcement has been issued. However the Act could have a significant impact on the Trust as it obliges public authorities to pro-actively publish datasets that it holds in an electronic format so that members of the public can re-use them. For the Trust this will mean that datasets will form part of the publication scheme via the Trust's internet site. The Act also stipulates that these datasets must be kept up to date. It is likely that this will impose a significant workload for departments that produce datasets on a regular basis. With this in mind, the IG department will review the Protection of Freedoms Act 2012 and advise the Trust on actions to ensure compliance with its requirements.

5.5 <u>Information Security & Information Risk Management Assurance</u>

These two requirements run in tandem and will be combined within the Project Plan for 2012/13.

5.5.1 The IG department will revisit Information Risk Management requirements across the organisation in light of v10 of the IG Toolkit and the recent internal audit recommendations.

5.5.3 Information risks will be reviewed and monitored by the Information Governance Steering Group. The SIRO will feed any Information risks/concerns into the Risk & Assurance sub-committee for discussion and escalation from local risk to corporate risk where appropriate.

5.5.4 The IG department will review and monitor IT business continuity as part of the Trust wide business continuity programme of work.

5.5.5 The IG department will devise a schedule for Trust systems to ensure that the appropriate system specific security documentation is complete and robust.

5.5.9 A series of audits are planned to be performed across the Trust to ensure that PC's and current Trust approved mobile equipment conform to Trust policy.

5.5.12 A requirement by the Department of Health is that all data that is used for "secondary use", (for reporting only), and not for direct patient care, must be pseudonymised, i.e. have all patient identifying information replaced with pseudonyms. As the Trust did not proceed with the proposed Management Information System (MIS) a Pseudonymisation working group has been established. The group will determine a process to help ensure that relevant systems have in place the ability to pseudonymise person-identifiable data for secondary use purposes by the end of 2012. Although this is a current requirement of the IG Toolkit, further national guidance is expected from Connecting for Health and the Information Commissioners Office around the use of anonymised and depersonalised information. In light of all new guidance, a full review on the handling of information for secondary use purposes will be undertaken and current action plans reviewed to reflect any changes to required compliance.

5.5.13 There is currently an overwhelming amount of requests being received for the use of tablet devices (iPad's / Android tablets etc) in both health related and admin / academic areas of the Trust. The Trust is currently reviewing solutions in relation to these devices to ensure that the security of network connections, patient identifiable, business sensitive and confidential information can be appropriately contained. With a secure framework in place the Trust can facilitate the use of such devices.

5.5.14 Similarly to tablet devices, requests to access social media are increasing within the Trust. There have been instances of inappropriate use of social media by staff from this Trust which has led to disciplinary action being taken which in some cases has resulted in dismissal. A Social Media Policy is being developed in conjunction with human resources and public relations. This will help to ensure that staff are aware of and comply with the appropriate guidance available when using social media in both a personal and a professional capacity.

5.5.15 The current agreement with Tees PCT for providing IT support within the Community setting will finish in March 2013. From this point it is anticipated that Community IT asset ownership will become a Trust responsibility. IG will need to look at exit arrangements working through how this will happen and any impact on the organisation.

5.6 Connecting for Health/National Programme for IT

5.6.1 Registration Authority

5.6.1.1 A business process options paper is currently being developed for a decision to be made on how to support Smartcard maintenance across the organisation. This may include the set-up of RA Workstations across divisions/locations to ensure staff are able to easily amend their Smartcard when necessary. The RA Manager will audit any activity on any workstations that are set up to ensure consistency and secure smartcard management is upheld across the organisation.

5.6.1.2 The RA function for community services is currently managed via a service level agreement with Middlesbrough PCT and North Yorkshire & Yorks PCT. Discussions are under way, however at present no decision has been confirmed with regards to how this service will run in the future.

5.6.2 Integrated Identity Management

5.6.2.1 The RA project team is producing a set of processes for new and existing staff which will incorporate the Smartcard/ESR interface. The position based access controls are continuously being uploaded and any anomalies identified. Each of these workstreams will contribute to the organisational achievement of Integrated Identity Management.

5.6.3 Summary Care Record Implementation

5.6.3.1 After a successful pilot of the Summary Care Record in 2011/12, the project team will consider options for implementing the SCR into non-emergency departments. The RA Manager will set up necessary workgroups and access rights which support role separation to ensure that SCRs are accessed securely and by those staff with a legitimate need.

5.6.3.2 The Privacy Officer role and the management of access alerts generated by the SCR will be evaluated and reported back to the organisation so that this role/responsibility can be aligned appropriately.

5.7 IG Training & Awareness

5.7.1 Information Governance training is mandated annually by the Department of Health. An IG trainer has been successfully appointed for 12 months in order to help the Trust reach level 3 on the IG Toolkit, seeing a minimum of 95% of staff IG trained. IG training can be accessed by either online training or by attendance at a delivered session.

5.7.2 In line with the NHS Informatics Plan all staff are now required to undertake IG training appropriate to their role through the NHS IG training tool e.g., Records Management, Clinical Record Keeping. Access to the training tool can be directly from the internet or via the National Learning Management System (NLMS), a module accessed via ESR. A Corporate decision on the use and rollout of the NMLS has yet to be finalised, in the meantime staff are still required to undertake the mandatory IG training either via the e-learning module or delivered session. Should the NLMS facility be rolled out, the Trust will see the benefit of staff having access not only to more specific aspects of IG training but to other required national training such as child protection.

5.7.3 Information governance is everyone’s responsibility. In order to achieve robust information management and a reduction in information incidents there needs to be assertive engagement and understanding across the Trust. Having access to up-to-date topic specific training will allow staff to undertake “advanced” training specific to their role within the organisation, helping to build on staff awareness and understanding of information governance. Guidance on role specific IG training now forms part of the mandatory training and development prospectus published by Human Resources.

5.7.4 The Trust Data Quality and Information Governance Forum acts as a medium for training and awareness session and allows constructive feedback from operational staff.

5.7.5 The IG Department will continue to produce the IG Eye quarterly bulletin which raises awareness of local and national IG issues/concerns. The bulletins function is to act as a "one stop update" on IG issues and hot topics for local team briefings.

5.8 Information Governance Department

5.8.1 The Information Governance Department will conduct an evaluation of the current systems in use for IG purposes including those still used by community services. The review will align current processes of work and ensure a single robust system, which is fit for purpose such as for the recording of FoIA requests, subject access requests, data flows, database registrations, Caldicott approvals and information assets.

5.8.2 The Head of Information Governance will review the department in line with the continuing developments of the IG agenda with obvious consideration for productivity and efficiency where necessary.

5.8.3 The IG department anticipates a significant role on numerous work streams for the Transforming the Care we Deliver Programme, but at the moment the areas and level of support is not defined.

6. Risks to Achievement

6.1 Achievement of Level 2 compliance on all IG Toolkit v10 standards across the integrated organisation.

6.2 As the Transforming the Care we Deliver Programme moves forward the information governance department will be involved in numerous work streams to ensure overall compliance with statutory and national requirements. It is not yet possible to estimate how resource intensive this workload will be and the impact on the management of IG operational issues. However with the introduction of divisional/directorate IG representatives it is possible that this risk may be reduced.

6.2 The integration of community services IG processes needs to be reviewed across the organisation to ensure that the Trust remains compliant with its statutory obligations. Key identified risk/considerations include:

1. Consistent approach to the management of information requests and archived information.
2. An integrated system for recording
    - Subject Access Request,
    - Freedom of Information Requests
    - Environmental Information Requests (EIR)
    - Information Assets
    - Dataflows/Audits
    - Community IT assets (transferred ownership from Tees PCT)

6.3 For community services all of the above are recorded electronically within a single system (MIDAS); however the Trust does not have electronic alternatives for all. The implications of moving away from a central IG repository to disparate systems will need further consideration by the organisation.

6.4 The Trust internet site/publication scheme is currently updated by divisions/directorates individually. There is currently no consistency when updates take place, resulting in either a lack of information or information out of date. Due to the impending ICO review of acute trusts publication schemes and the enactment of the Protection of Freedoms Act 2012, the organisation needs to ensure that the publication scheme criteria is met and that all information required via the internet is up-to-date. Non-conforming organisations will be contacted by the ICO directly. The Trust therefore needs to ensure that its information for the public is published routinely and consistently, for the benefit of its patients, clients and reputation.

6.5 Although the IG department has recruited a temporary IG trainer, the Trust still relies on staff to take responsibility for completing the training themselves. Training will be monitored and reported to divisional managers and corporate directors to ensure that IG training is undertaken in order to reach the continuous 95% level 2 requirement. A report on training was presented to the R& Assurance sub-group on 12th June 2012 confirming current Trust compliance at 56% This standard will be level 1 compliant for the benchmark submission at 31st July 2012 (see appendix C)

6.6 Information risk management, including asset ownership, like any culture change has taken time to embed into the organisation. Accountable staff need to ensure that information risk and asset management/ownership responsibilities are administered effectively and not seen as an IT/IG responsibility. An appropriate system and process needs to be in place to ensure the robust management of Trust information assets.

6.7 As the Trust did not proceed with the proposed Management Information System (MIS) a Pseudonymisation Working Group has been established and is currently helping to determine a process to help ensure that relevant systems have the ability to pseudonymise person-identifiable data for secondary use purposes. This may require additional development from system suppliers which if needed is likely to incur additional costs. Additional guidance around anonymisation and de-identification is also expected shortly from Connecting for Health and the Information Commissioner's Office, giving a "pause" effect to the current work underway. A delayed delivery of this guidance may impact on the working group to review and apply the required actions/processes across the Trust. This standard will be level 1 compliant for the benchmark submission at 31st July 2012 (see appendix C)

6.8 The Trust will shortly be out to tender for a mobile device management solution to ensure that the use of devices such as tablets etc., can achieve compliance with statutory and national requirements on information security. The Trust understands that the need for mobile working is ever increasing; however in such times when information security is paramount it is vital that the solution selected by the Trust offers the required security compliance.

6.8 The IG agenda is large and complex with ever increasing demand on the service. *Transforming the Care we Deliver Programme* and Trust efficiencies are being taken into consideration within the IG Department and as a consequence may affect the delivery of the IG agenda, reflecting in the Trust's overall IG compliance score for 2012/13.

7. Summary

7.1 This report sets out what has been achieved within the IG Programme for 2011/12. This year has again seen a rapid increase in demand on Trust resources dedicated to the IG programme and the team has worked hard to ensure that the Trust has kept up with the pace of the demands of the National Information Governance agenda, in addition to the day to day operational aspects of IG.

7.2 More importantly this report sets out a work programme to further enhance a robust IG framework within South Tees Hospitals NHS Foundation Trust for 2012/13. The year's priorities focus further on information risk management and ensuring that processes are in place to support patient rights, confidentiality and data security and accessibility.

7.3 As the visibility of IG is raised, so are the demands on the service. Activity is constantly increasing and the organisation needs to ensure that information governance is managed in a robust way within work areas and not seen as something that is the sole responsibility of the IG Department.

7.4 Information Governance forms part of the Integrated Governance Framework and the one thing that is certain, is that this already large and complex agenda, still gains momentum. Public interest will continue to rise through the media reporting of adverse events, as seen in the first NHS monetary penalties for data loss/breach. Going forward, the IG team are monitoring how the ICO applies its Regulatory Powers (particularly to the NHS) with regards to penalty notices for data loss incidents and where required, continue to apply the learning to ensure risk mitigation within South Tees NHS Foundation Trust.

7.5 The Board of Directors is asked to:

- note IG progress in 2011/12
- approve the High Level Project Plan (Appendix B)
- approve the required IG Toolkit baseline score for July 31st 2012 submission (Appendix C)

N Huntley
Head of Information Governance

June 2012

(Appendix A)

GLOSSARY

Abbreviation	Term
CfH	Connecting for Health
CG	Caldicott Guardian
CRG	Care Record Guarantee
CRS	Care Records Service
Data Handling Review	A review of data handling across government departments following a data loss by Her Majesty's Revenue and Customs (HMRC)
DATAC	Durham and Tees Valley Audit Consortium
e-GIF	e-Government Interoperability Framework - Levels 0-3. e-GIF level 3 compliant - identity proven 'beyond reasonable doubt', evidenced by three forms of identification.
Encryption	The conversion of data into an unreadable coded format
ESR	Electronic Staff Record
HMRC	Her Majesty's Revenue and Customs
IAA	Information Asset administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IGAF	Information Governance Assurance Framework
IGAP	Information Governance Assurance Programme
ISA	Information Sharing Agreement
IT	Information Technology
N3	New National Network – the NHS broadband networking service
NHSNET	National Health Service Network
NIGB	National Information Governance Board
NLMS	National Learning & Management System (access via ESR)
PC	Personal Computer
PDA	Personal digital assistant
RA	Registration Authority – the Trust's arrangement for the issuing and management of smartcards
RAM	Registration Authority Manager
SCR	Summary Care Record
Sealed Envelope	**Electronic** sensitive information sealed from view at the request of patient or clinician
SIRO	Senior Information Risk Owner
SMARTCARD	A plastic card used to control access to the NHS Care Records Service
SOC	Statement of Compliance
SUI	Serious Untoward Incident
USB	Universal Serial BUS – device that holds data and can be connected to a computer
SOP	Trust Standard Operating Procedure

Agenda Item Number 10.1

(Appendix B)

Information Governance High Level Project Plan – 2012/13

Key Driver	Key Actions	Responsibility	Timescale
Audit & Monitoring	Update Work Programme for IG Toolkit v10	Head of Information Governance	Jul 2012 Oct 2012 Mar 2013
	Work with identified requirement owners to support and evidence IG Toolkit scores.	Information Governance Specialists	Mar 2013
	Audit North to audit IG Toolkit scores and evidence	Head of Information Governance/Audit North	Mar 2013
	Verification of IG Toolkit scores and evidence	Head of Information Governance / Head of Financial Governance & Control	Mar 2013
	Undertake PC continuous testing audits	Deputy IG Manager	Jan 2013
	Develop Health Assure for collation and monitoring of IG evidence and attainment levels	Head of IG	Mar 2013
	Review overarching IG policy to ensure appropriate and robust IG framework across the Trust IG groups in light of IG agenda and Trust Information Strategy	Head of IG	Aug 2013
Legislation, National standards & Policy	Review/develop Information Governance Policies& Standard Operating Procedures	IG team	Ongoing
	Align other National Standards into IG Toolkit Work Programme i.e. SfBH / IGAP / NHS Operating Framework	Head of Information Governance	Mar 2013
	Review of the Protection of Freedoms Act 2012 and advise the Trust on compliance requirements	Head of IG IG Specialist Records Management	Aug 2013
	To aim for level 3 scoring on all Information governance Toolkit Standards (Minimum level 2 required to satisfy Monitor and Operating Framework requirements)	Head of Information Governance	Mar 2013
Confidentiality & Data protection Assurance	Review of the Data Protection Act, subject Access Request Processes.	Head of Information Governance IG Specialist - DP	~~Oct 2011~~ c/f to 2012/13
	Trust Data Protection Audit • Action against 2011/12 survey results • 2012/13 DPA survey • Divisional/Directorate DPA spot checks • Service user DPA satisfaction spot checks	IG Specialist – Data Protection	Jan 2013
	Review Trust Information Sharing agreements and guidance for staff on information sharing	Head of IG IG Specialist DP	Nov 2012
	Review of Information Governance Incident Management including coding of Incidents	Head of Information Governance / IG Specialists	~~Oct 2011~~ C/f to 2012/13

Information Governance High Level Project Plan – 2012/13

Key Driver	Key Actions	Responsibility	Timescale
Corporate Information Management	To work with Divisional IG representatives to audit and register divisional information assets	IG Specialist – Records Management	Mar 2013
	To advise and monitor divisions of their input into the Trust's publication scheme	IG Specialist – Records Management	Mar 2013
	To review and improve the Trust's corporate system for the handling and monitoring of FOI requests to ensure compliance with the statutory 20 day timeframe.	IG Specialist – Records Management	Oct 2012
Information Security & Information Risk Management Assurance	Work with and support System IAA's to ensure the required system documentation is in place.	Deputy IG Manager	~~Feb 2012~~ c/f 2012/13
	To undertake IT Business Continuity as part of the Trustwide Business Continuity Programme of work	Deputy IG Manager	~~Feb 2012~~ c/f 2012/13
	To advise and support the Trust on Mobile Device Management	Deputy IG Manager	Mar 2013
	To advise and support the Trust on the Management and use of its social media.	Deputy IG Manager	Mar 2013
	Revisit and support Divisions and Directorates on Information Risk management requirements across the Trust	Deputy IG Manager	Nov 2012
	To advise and support the Information Department on Pseudonymisation of data for secondary use purposes.	Deputy IG Manager	Dec 2012
	Review exit arrangements around the transfer of Community IT assets to South Tees FT.	Deputy IG Manager/Head of IG	Dec 2012
Connecting for Health & National Programme for IT Registration Authority	Roll-out of Summary Care Record (SCR)	Project Manager / RA Manager	Ongoing
	Transfer of SystmOne Units from PCTs to South Tees	Project Manager	Nov 2012
	Review of on-going smartcard maintenance and support across the Trust	IG Specialist – Registration Authority	Nov 2012
	Review and appropriate alignment of "Privacy Officer" role with the Trust	IG Specialist – Registration Authority	Nov 2012
IG Training & Awareness	Trustwide awareness on IG including local and national issues	IG Specialists	Ongoing
	Review IG mandatory training requirements to ensure • All staff (min 95%) complete annual training • IG forms part of the corporate TNA to ensure compliance with IG toolkit requirements.	IG Trainer	Mar 2012
IG Department	Review the department in line with the continuing developments of the IG agenda with obvious consideration for productivity and efficiency.	Head of Information Governance	Sep 2012

Agenda Item Number 10.1

(Appendix C)

2012/13 Proposed Baseline Score for South Tees NHS Foundation Trust

Req No	Description	Attainment Level ?
Information Governance Management		
10-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Level 3 ✓
10-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Level 3 ✓
10-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Level 2 ✓
10-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Level 3 ✓
10-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Level 1 ✗
Confidentiality and Data Protection Assurance		
10-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Level 3 ✓
10-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	Level 3 ✓
10-202	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	Level 2 ✓
10-203	Individuals are informed about the proposed uses of their personal information	Level 2 ✓
10-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Level 2 ✓
10-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Level 3 ✓
10-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Level 2 ✓
10-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Level 3 ✓
10-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	Level 2 ✓
Information Security Assurance		
10-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Level 3 ✓
10-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Level 2 ✓

10-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Level 2 ✓
10-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Level 3 ✓
10-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Level 3 ✓
10-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	Level 2 ✓
10-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Level 2 ✓
10-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers	Level 2 ✓
10-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place	Level 2 ✓
10-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Level 2 ✓
10-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Level 2 ✓
10-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Level 2 ✓
10-314	Policy and procedures ensure that mobile computing and teleworking are secure	Level 2 ✓
10-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Level 2 ✓
10-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Level 1 ✗
Clinical Information Assurance		
10-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Level 2 ✓
10-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Level 2 ✓
10-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	Level 2 ✓
10-404	A multi-professional audit of clinical records across all specialties has been undertaken	Level 2 ✓
10-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Level 2 ✓
Secondary Use Assurance		
10-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Level 2 ✓

10-502	External data quality reports are used for monitoring and improving data quality	Level 2 ✓
10-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained	Level 2 ✓
10-505	An audit of clinical coding, based on national standards, has been undertaken by a NHS Classifications Service approved clinical coding auditor within the last 12 months	Level 2 ✓
10-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Level 2 ✓
10-507	The Completeness and Validity check for data has been completed and passed	Level 2 ✓
10-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Level 2 ✓
10-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards	Level 2 ✓
Corporate Information Assurance		
10-601	Documented and implemented procedures are in place for the effective management of corporate records	Level 2 ✓
10-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Level 3 ✓
10-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Level 2 ✓