Derby City Council

AUDIT AND ACCOUNTS COMMITTEE
8 December 2014

ITEM 13

Report of the Head of Governance & Assurance

Compliance with NHS Information Governance Toolkit - Update

SUMMARY

1.1 This report provides an update to Committee on the Council’s progress with obtaining compliance with the NHS Information Governance Toolkit.

RECOMMENDATION

2.1 To seek updates on progress with the actions in appendix 2 at future meetings.

REASONS FOR RECOMMENDATION

3.1 The Audit and Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

SUPPORTING INFORMATION

4.1 At it's meeting on 24 September 2014, Committee received an update on progress in achieving compliance with the NHS Information governance toolkit. The Director of Public Health attended the meeting to outline the key implications on his service for non-compliance with the toolkit.

4.2 It was agreed that a further report would be brought back to this Committee to outline the work that was being undertaken to work towards compliance.

4.3 Included with the report to Committee was an external analysis of the level of compliance the council can demonstrate with the IG Toolkit. The Director of Information Systems, as Acting Senior Information Risk Owner (SIRO), has reviewed each of the recommendations in the report and drawn up suggested actions to address these. These are shown in Appendix 2.

4.4. A re-structure in the Information Governance team has created a new post of Information Governance Policy Officer. One of the roles of this post will be to support the Council's work on achieving compliance with the Toolkit.

4.5 A further issue has arisen that makes it imperative that the Council continues to work towards compliance with the NHS IG Toolkit. The Health & Social Care Information Centre (HSCIC) has recently written to customers that have already signed an existing Data Sharing or Data Re Use agreement to cover the data they receive from the HSCIC. The HSCIC now needs the Council to complete the necessary parts of the new Data Sharing Framework Contract. Before the HSCIC will enter into the new contract with you, it needs to be assured that the Council has appropriate information governance controls in place to receive health and social care data.

4.6 The HSCIC expects that all customers should be able to demonstrate that they comply with the IG Toolkit or are certified to ISO27001. If a customer is not able to demonstrate either of these requirements, then they will need to provide details of their security policies. However, the HSCIC will only be able to agree a contract with such organisations for one year, rather than the standard three year term. Because the Council is not yet fully compliant with the toolkit and is not certified to ISO27001, we will need to demonstrate that we have appropriate information governance controls in place if Public Health is to be able to continue to share data with the HSCIC. The Senior Public Health Analyst is currently gathering evidence in support of this.

OTHER OPTIONS CONSIDERED

5.1 N/A

This report has been approved by the following officers:

Legal officer	n/a
Financial officer	n/a
Human Resources officer	n/a
Estates/Property officer	n/a
Service Director(s)	n/a
Other(s)	Chief Officer Group

For more information contact:	Richard Boneham, Head of Governance and Assurance, 01332 643280 richard.boneham@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 – Actions to address areas of non-compliance

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 None directly arising.

Legal

2.1 None directly arising

Personnel

3.1 None directly arising

IT

4.1 As detailed in the action plan in appendix 2

Equalities Impact

5.1 None directly arising

Health and Safety

6.1 None directly arising

Environmental Sustainability

7.1 None directly arising

Property and Asset Management

8.1 None directly arising

Risk Management

9.1 Non-compliance with the toolkit will mean that Public Health will not be able to access the data it requires.

Corporate objectives and priorities for change

10.1 None directly arising.

Appendi
x 2

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
IG Framework			
12-144 There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	1 Further improvement to defining governance roles, as planned, following departure of Information Governance Manager	COG Report and Action plan to start addressing Action 1	SIRO (Director of ICT) and Director of legal and Democratic Services
	2 Job descriptions should be updated to set out roles and responsibilities and how these will be linked to the annual submission of the IG toolkit	Need Role descriptions to be appended to job descriptions for SIRO, Caldicott Guardian and all Information Asset Owners	IG Policy Officer and HR
	3 A resource plan to deliver the annual submission of the IG toolkit should be drawn up and presented for the approval of the IGB. This should set out dedicated budgets - including specialist training for certain roles - for all key staff involved in the IG agenda below those at Board or most senior levels. This may include an IG officer, Data Protection Officer, Information Security Officer, Freedom of Information Manager, Corporate and Clinical Governance leads or Data quality leads. High level plans for expenditure in-year should also be identified, including outsourcing to external resources or con-tractors.	Need to get some examples of time and resource effort required and then consider how we can manage this using existing resources and/or with additional resources	Assistant Director of Public health (Corporate) to get examples then IG Board to review
	4 The Caldicott Guardian should be registered on the national register.	Completed	Completed
12-145 There are approved and comprehensive	1 A Corporate Governance Policy should be developed	Review and enhance Existing Policy – This is Information Governance	SIRO and IG Policy Officer to IG Board

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
Information Governance Policies with associated strategies and/or improvement plans			
	2 Develop an Information Quality policy. (An Information Quality policy is dated 2008 and no longer reflecting the current position of the Council).	Review current policy and map this to IG Toolkit expectations ; review all other policies which may also be out of date including each listed above	IG Policy Officer
	3 IG Action Plan recommendations need to be updated especially around a number of key areas, such as development of the IAR	a) Review outstanding ICO action plan and IG Toolkit plan and develop new plan b) Establish Template and collection/collation requirements for Information Asset Register	IG Board – IG Policy Officer IG Policy Officer and Information Asset Owners (IAO's)
	4 Consideration should also be given to extending the IG plan or devising separate plans for the variety of year-on-year information governance improvements. For example, for information/data quality, IAR updates etc.	Agree a review cycle – suggest quarterly updates by IAO's with half yearly review by IG Board	IG Board and IAO's
12-146 Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	1 The Procurement and Legal teams should perform a comprehensive review of all existing contracts to assess whether appropriate contractual clauses covering compliance with IG have been drafted, and produce a report on the findings of the review. This may be performed in conjunction with the planned value for money reviews of all contracts.	a) Check do we have such a clause if not need to draft one b) Check all new tenders where supplier will have access to information insert such (Not all contracts) c) Consider how use of framework contracts may or may not apply such d) Review contracts and identify which provide supplier with access to information assets	Head of Procurement /Principal lawyer Procurement team Legal Information Asset Owners (IAO's)
	2 IA should consider reviewing this process to make sure all relevant contracts are appropriately worded and reflect the requirements of the IG Toolkit and wider governance agenda.	a) IAR should establish which contracts provide suppliers with access to Information Assets b) For each supplier need statement of compliance to be recorded – possibly as a schedule to each contract c) Need to consider if/how to audit for compliance	IG Policy Officer and IAO's On each contract Internal Audit to consider
12-147 Employment contracts which include compliance with information	1 Documented action plan for raising awareness of and compliance with information governance standards should be produced to make sure that all policies and associated procedures are being	This was covered in the COG report and needs to form part of induction procedures and MIP's – ask HR	Director of ICT to liaise with HR

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
governance standards are in place for all individuals carrying out work on behalf of the organisation.	read and adhered to		
	2 The induction training and staff code of conduct should be reviewed to make that the existing pro-cesses can make sure staff are aware of the latest policies and improvements and read and under-stand them	Need to review with HR – note has always been resistance to adding explicit information governance issues to these previously	Director of ICT to liaise with HR
	3 A documented vetting procedure should be developed so that all new staff are appropriately vetted, trained and provided with guidelines to ensure they are aware of their obligations for IG before they start handling person identifiable information	We use the PSN guidance to determine which staff we vet for disclosure checks; the only way this could be extended would be to introduce a mandatory test to be carried out by line managers as part of the probation period for staff and in the first week for agency staff. Need HR to advise.	Director of ICT to liaise with HR
	4 All employment contracts should contain appropriate IG clauses	We need to draft these – some examples would help if we can source such form others. Then agree with HR and will be a change to terms and conditions which the need approving by CoSWP. JCC and Personnel Committee approval	Assistant Director of public health (Corporate) and Director of ICT to seek examples; Director of ICT to liaise with HR.
12-148 The training needs of all staff are assessed in relation to Information Governance requirements and they are all appropriately trained	* Renew PSN Certificate OR steps 1,2 and 3 below	PSN Certificate is being renewed but should still pursue other actions to ensure more robust approach	Director of ICT and IS Dep't
	1 Responsibility should be assigned to an individual or team to develop the information governance training programme.	Will be assigned to IG Policy Officer (New post)	IG Policy Officer/Head of Governance and Assurance
	2 A training needs analysis review should be performed that highlights how existing training is	Would need central co-ordination between IG Policy Officer and HR and support of all Line	IG Policy Officer and HR

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	meeting required IG needs.	managers, adding an Information Governance statement to MIP reviews would help (we have asked for this before but HR prefer not to add too many things to the MIP checklist)	
	3 Following this analysis, a dedicated IG training programme should be developed to make sure all staff have the training they require for their specific roles. (Some roles will have a greater focus on IG related matters than others. The training should be targeted to be appropriate and also cost effective).	IG Policy Officer with support of HR Organisation and Development team	IG Policy Officer and HR
Confidentiality and Data Protection Assurance			
12-251 The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation’s assessed need	1 All Data Protection Officers should have specialist training and appropriate qualifications.	Need to understand what they mean by Data Protection Officers – who these are and how many	Head of Governance and Assurance
	2 Produce a written plan including the details of the job role(s) or a responsible group that will form the Caldicott function, with an associated improvement plan. This should be approved by the IGB.	Need to check NHS IG Toolkit and what is meant by a Caldicott function as opposed to a Caldicott Guardian – an ex-ample Caldicott function would be very useful	Assistant Director of public health (Corporate) and Head of Governance and Assurance
12-252 Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	The Staff Code of Conduct needs to be reviewed to in-corporate the following: • The legal framework and the circumstances under which confidential information can be disclosed; • The Caldicott Principles revised September 2013; • The Social Care Record Guarantee for England;	We would not normally add these to the code of conduct; this may more need to make up a revised Information Security policy to which the code of conduct explicitly refers.	IG Policy Officer & Head of Governance and Assurance and HR Department

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	• HSCIC 'A guide to confidentiality in health and social care: Treating confidential information with respect'; • Care professionals must also comply with the codes of practice of their respective professions; • The systems and processes for protecting personal information. This will include any safe haven proce-dures, any information sharing protocols agreed with external organisations, encryption requirements for mobile devices etc; • Who to approach within the organisation for assis-tance and advice on disclosure issues. Although there may be a range of individuals who can assist with difficult issues – Information Governance leads, Caldicott Guardians, Senior Information Risk Owners, Data Protection leads etc. – it is important that the Council provides clear signposts to its staff; and • Possible sanctions for breach of confidentiality or data loss. The Council should ensure that all staff members are aware of the possible disciplinary sanctions for failure to comply with their responsibilities, e.g. deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal information electronically without encrypting it, etc.		
12-253 Personal information is shared for care but 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	1 Provide documented and approved guidelines at appropriate points in the Council on when it is both lawful and appropriate to share confidential personal information and on respecting service user wishes. All staff members should be effectively informed about the need to comply with them.	We need specific policies regarding health and social care to cover this requirement that need to be added to i-derby under both the Information Governance section and under respective departmental pages. An example we could adapt and adopt would help.	

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
disclosure of confidential personal information are appropriately respected.			
12-254 Individuals are informed about the proposed uses of their personal information	1 A formal communications strategy to provide more comprehensive information services to users should be established.	a) Need to review, consolidate update and re-publish all such materials and appoint someone to be responsible for maintaining these in future. b) Need to agree a communication strategy with the communications team to ensure regular briefings are issued	IG Policy Officer IG Policy Officer & Comms team
	2 All staff members should then be effectively informed about the existence of the updated materials.	Need to include updates in team brief cascades, through in touch and in team meetings	IG Policy Officer & Comms team
12-255 Where required, protocols governing the routine sharing of personal information have been agreed with other organisations.	1 Responsibility for identifying all organisations with which personal information is routinely and regularly shared, and developing suitable information sharing protocols, should be assigned to an individual.	Information Asset Owners in each directorate need to both map these into a chart and to ensure we have relevant data sharing agreements. These should then be collated centrally by the Information Governance Team.	ALL Information Asset Owners, ALL DMT's and IG Policy Officer
	2 Draw up a list of information sharing partners that are unable to demonstrate they are meeting the required information governance performance (e.g. name/type of organisation, the information required to be shared, the purpose of the sharing).	All Information Asset Owners to identify these and report to the IG Team and to the IG Board.	ALL Information Asset Owners, IG Policy Officer and IG Board
	3 There is a high level protocol setting out the basic information governance principles that each sharing partner will comply with that has been approved by senior management. NB - until the Council itself reaches level 2 of the IG Toolkit, there is every likelihood that it will be asked to provide assurances to other organisations. This work should be considered as part of the resource implication assessment for the IG framework, as referenced above.	IG Policy officer to prepare based on existing agreements, IG Board, COG and relevant Cabinet Member to agree and then publish on i-Derby	IG Policy Officer , IG Board

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
12-256 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	* Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT /IS department
	1 Update the existing project management frame-work so that all new projects or significant changes are required to consider information governance risks and controls.	This is already a requirement for all new IS projects and embedded within the IS business case approval process; would help to also amend the risk management handbook.	Head of Governance and Assurance
Information Security Assurance			
12-371 The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	* Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT/IS Department
	1 Document a plan for Information Security Assurance, approved by the IGB, that supports the necessary work related to information security management. This should include details of the responsible job role(s) and reporting structure.	We have an IS Policy but yes reviewing the role and copying and expanding on the report recently agreed by COG would enhance this	IG Policy Officer and SIRO (Director of ICT)
	2 Responsibility for supporting the Information Security agenda should be identified in various staff roles co-ordinated by the Information	As Action 1b this is now identified in the COG report but need to add to the specific job roles for the people/posts identified	IG Policy Officer and HR Department

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	Security Manager/Officer and includes corporate responsibility at the IGB level.		
12-372 A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	* Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT/IS Department
	1 Document an Information Risk Assessment and Management Programme, and establish associated strategies, policies and procedures. The Programme should be approved by the IGB.	Not clear what is meant by such a programme rather than a policy, this may be the work tasked to the relevant officers as per the COG report and/or by the IG Boar d- in effect an annual IG plan	IG Board and SIRO, Head of Governance and Assurance
	2 Update the Council's risk register with this information	The IG risk register entries are maintained by the IG team	Head of Governance and Assurance
	3 The results of information risk assessments and recommendations should be reported to the IGB.	For the annual plan and review this will be the IG team for new projects it will be the project sponsor	Head of Governance and Assurance
	4 Internal Audit should review the risk assessment programme on a regular basis to assess its effectiveness.	I believe this is in the audit plan – if not we can add	Head of Governance and Assurance
12-373 There are documented information security incident / event reporting and management procedures that are accessible to all staff	1 The Caldicott Guardian should ensure that she is aware of all information security incidents involving unauthorised disclosure of confidential service user information.	Under new arrangements these will be reported to AHH and CYP DMT's and therefore to the Caldicott guardian	IG Team
	2 These incidents, including near misses, need to be promptly reported to the SIRO and the relevant Information Asset Owner for consideration of any necessary actions	Again following COG report this has been agreed and we need all incidents sent to the SIRO, Caldicott Guardian and the respective DMT and IAO for that directorate, To support actions 1 and 2 a new e reporting form	IG Team Head of Governance and

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
		will be produced to make it easier for such to be submitted and this form needs to include a tick box for caldicott applies. IT also needs a field for directorate. The form will consolidate existing processes and be embedded within a new form for all serious incidents as well as a stand- alone form.	Assurance
	3 The Council should ensure that responsibility for man-aging information security incident/events is documented within the IG Lead/SIRO/IAO and other relevant job descriptions. Responsibilities should also be clearly explained in any contract or agreements with other organisations affected.	Need to ensure this is included in revised job role definitions and in standard contract clauses. ((Note this overlaps elsewhere)	IG Policy Officer and HR Department IG Policy Officer & Legal/Procurement
	4 Documented reporting, investigating and managing information security events procedures need to be established. The procedures should be approved by the IGB.	These do exist but do need improving and updating, this is reflected in the COG report but needs enacting	IG Policy Officer
	5 Staff briefings on this matter should take place or inclusion of information security reporting on the e-learning portal.	This repeats earlier recommendations this will be included on e-Portal and through team brief cascade and In Touch mailings	IG Policy Officer to produce, Comms Team to publish
	6 As part of the work to review existing contracts - to be started - consider information security alongside IG requirements.	Information security is already a mandatory consideration for all IS contracts but seeking to amend procurement regulations to make this more explicit. For no-IS contracts including agency staffing need to ensure contract owners are aware and cover this.	Director of ICT for IS Contracts Procurement team for other contracts
12-374 Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights	* Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT and IS department

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
are in place for all users of these systems			
	1 Responsibility for defining and documenting requirements for both system and user access controls should be assigned to IAOs.	Irrespective of PSN certification this is a task that should be completed and needs doing between IAO's and system owners/administrators – this is similar to an ICO action still not completed. This should be part of the system documentation.	IAO's, System Owners and System Administrators
	2 IAOs should ensure that there are approved access controls in place for each key information asset under their control	Irrespective of PSN certification this is a task that should be completed and needs doing between IAO's and system owners/administrators – this is similar to an ICO action still not completed. This should be part of the system documentation.	IAO's, System Owners and System Administrators
12-375 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	Renew Public Services Network Code of Connection Certificate. OR	Information Systems department to achieve PSN certification	Director of ICT and IS department
	1 Document a plan to ensure transfers, of person identifiable and sensitive information, to and from the Council are risk managed and adequately secure.	For each type of person identifiable data we need a record of what the data is and who it may be sent to and in what format. Where the format is electronic we should only use either the egress switch secure data sharing system (already widely used for social care) or secure PSN compliance emails (used by benefits) or CJSM mail (used for youth offending casework). For no electronic transfer we need clear policy and guidance on the use of secure recorded delivery mailings. We need a corporate policy set by the IG Board and local working practices established jointly by the respective IAO and the data owners.	IG Policy Officer and IG Board Information Asset Owners and Data Owners in each department

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	2 Routine flows of person identifiable and sensitive information in all areas should be identified, mapped and recorded. Risks should be identified and recorded. Action should be taken immediately where high risks are found. This work should be reported to the IGB.	IAO's need to map this as part of the information asset register and with the accompanying risk assessment for each incoming, in transit and outgoing data flow. We need some templates to support such.	Information Asset owners supported by the IG Policy Officer
	3 Up to date information transfer agreements should be established with partner organisations.	Each data owner agreeing to a transfer agreement needs to ensure this, copy to their Information Asset Owner who will forward for adding to the corporate register.	Data Owners, Information Asset owners and IG Team.
12-376 Business continuity plans are up to date and tested for all critical information assets (e.g. data processing facilities, communications services and data) and service - specific measures are in place	1 Document an organisation-wide Business Continuity strategy and programme which sets out the approach to Business Continuity Management and responsibilities of the Information Asset Owners and relevant staff. This should be approved by the IGB.	This is documented and is maintained by Emergency planning – the finding is incorrect. We may however need to review this as it does not refer to Information Asset owners.	IG Board, Business Continuity Plan holders and Information Asset Owners
	2 All business critical systems, including those provided by service contract or agreement, have been assessed by the relevant IAO and they are aware of the effect that disruption may have and the need to develop Business Continuity Plans for each of their assets. The plans should be approved by the IGB.	This is not a role for the IG Board it is a role for each Directorate Management Teams and the corporate Business Continuity Board, there is a danger of duplication or inconsistency.	DMT's and Business Continuity Plan holders
	3 The documented strategy and associated programme should appear in the relevant Information Asset Register when this has been completed	No – the Information Asset Register should have reference to the corporate business continuity strategy and plan - duplicating this would not help	IG Policy Officer to liaise with Emergency Planning
	4 IAOs should develop system level security policies that include all aspects of back up arrangements for the key assets.	Agree that backup plans including frequency, type (full or incremental) and number of generations held should be documented; this is more for system owners/administrators and can be supported by the IS department with a template. Yes these should be copied to Information Asset	System Owners and Administrators supported by IS department.

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
		Owners	
12-377 Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.	See 12-372 for further information and recommended actions.	See 12-372 for further recommended actions.	
12-378 Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Renew Public Services Network Code of Connection certificate. OR	Information Systems department to achieve PSN certification	Director of ICT and IS department
	1 Document controls and procedures to mitigate against malware risks and fully implement across the Council. This includes a documented information asset register.	a) The Information Asset Register is in production and we need to review and improve progress. b) The malware controls are in place but a revised policy documents may enhance this.	Information Asset Owners & IG Policy Officer IS Department
	2 Assess whether malware solutions and controls are working through the use of system reports.	Not clear what these means if it refers to logs produced by intrusion prevention and detection need to check we have these; if not need clarification !	IS Department – Technical Architect
12-379 Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT and IS department
	1 A network security policy needs to be produced for each ICT network and systems	We have such a security policy and we will not and should not delegate this down to information	IS Department – Technical Architect

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	approved by the relevant IAO.	asset owners, such would be counter to best practice. The correct action is to ensure the policy meets required compliance regime standards	
	2 IAOs responsible for ICT networks should perform reviews of information security risks in relation to those networks, and the controls and procedures required to mitigate these risks in accordance with the Network Security Policy.	Again this recommendation is flawed and will not be enacted. The correct action is to ensure compliance with regimes including the regular undertaking of penetration and compliance checks – all managed by the IS Department.	IS Department – Technical Architect
12-380 Policy and procedures ensure that mobile computing and teleworking are secure	Renew PSN Certificate OR	Information Systems department to achieve PSN certification	Director of ICT and IS department
	1 Document procedures for mobile working or teleworking that provide guidelines for staff on expected behaviours.	These were documented as part of the Derby workstyle – and in the mobile computing policy – yes these many need review and update.	IS Department and IG Policy Officer
	2 Assess whether robust remote access solution(s) are in line with the PSN requirements	This is part of PSN compliance regime.	IS Department – Technical Architect
12-381 There is an information asset register that includes all key information, software, hardware and services	1 IAOs should establish a register for all information assets - software, physical and services - for their respective areas and assign updating responsibility to a named individual.	This is in progress but needs checking and needs monitoring by the new IG Policy officer post.	Information Asset Owners and IG Policy Officer – signed off by each DMT
12-382 All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	* Renew PSN Certification OR	Information Systems department to achieve PSN certification	Director of ICT and IS department
	1 Compile local IARs using flow-mapping and IAR template completed by AHH	For each Information Asset Owner in each Directorate – then to be collated into a central Information Asset Register by the IG team.	Information Asset Owners and IG Team
	2 A clear description of the safeguards that have been deployed should be included within the Information Asset Register.	A common safeguard document covering technical and organizational safeguards to be developed and maintained with additional local safeguards added by respective Information Asset Owners	IG Policy Officer, IS Technical Architect and each Information Asset Owner

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
	3 IA should review the process to be followed to compile the IAR. This should review the plan to identify any relevant information assets that the Council was previously unaware of has been implemented and there is a high degree of confidence that all such assets have been identified and secured. This report should to taken to the IGB.	IG policy officer to collate into a central Information Asset Register and then do a gap analysis – can compare to other sources such as software systems in use, EDRMS workspaces etc/	IG Policy Officer and IG Board
12-383 The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	1 Document Project plan(s) for safe havens and implementation of the pseudonymisation/anonymisation plan. (The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure the care provided. The Anonymisation Code of Practice published by the Information Commissioners Office provides guidance to any organisation which wants to turn personal data into anonymised information for research or other data analysis purposes. There is also an Information Standards Board for Health and Social Care information standard which provides an agreed and standardised approach, grounded in the law (standard ISB 1523).	Need to review the ICO guidance and then identify who in the Council has a need for such and ensure this is understood and the relevant techniques, policies and tools are in place. Mainly applies to health and social care which should be a priority but could also apply elsewhere	Information Asset Owners in health and social care and IG Policy Officer.
Care Records Assurance			
12-441 The Information Governance agenda is supported by adequate information quality and	1 Update Data Quality Policy. This should be approved by the IGB and issue to all relevant staff.	Review and update policy then publish on i-Derby	IG Policy Officer, Performance team

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
records management skills, knowledge and experience			
	2 Responsibilities for Information Quality and Records Management Assurance should be identified in various staff roles co-ordinated by the lead managers/officers and include corporate responsibility at a senior management level.	Needs standard clauses that can be used in job descriptions and we can use COG report that identifies key posts that need such	IG Policy Officer, HR department
	3 Training should be provided where deemed necessary, depending upon role.	Need to consider what, if any, additional training is needed for various roles especially those identified in the COG report and embed this within MIP process and training plans	IG Board
12-442 There is consistent and comprehensive use of the NHS Number in line with National Policy requirements	It is understood that a Project on the NHS Number Use has been completed by the Council. However, evidence for its completion has not been seen as part of this re-view. If the relevant documentation is available, the score could be amended to a 2.	Check on use of NHS project, has this been implemented if so just need evidence, if not need to review.	AHH to advise further
12-443 Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	1 Responsibility should be assigned to an individual or group to develop and implement procedures for ensuring the accuracy of service user information on all systems and/or records that support the provision of care	Believe in AHH this role exists and is undertaken by Head of Business Intelligence and colleagues; need to check if this also happens for public health function and in CYP directorate. If not need to address this in those areas.	AHH and CYP Information Asset Owners
	2. Data collection and validation activities should be regularly monitored. All staff collecting and recording data are effectively trained to do so and dedicated staff take appropriate action where errors and omissions are identified.	Need to check what data validation procedures are built into data entry on systems like liquidlogic and others that hold care data and need to keep records of relevant staff training both as part of new system implementation and for new starters or refresher training for staff.	AHH and CYP Information Asset Owners
12-444 Procedures are in place for monitoring the availability of paper	1 Document procedures for monitoring paper service user record availability, which includes measures to track records removed from the	Need to check what procedures exist in both AHH and CYP and what procedures exist in business support in respect of paper documents they	AHH and CYP Information Asset Owners, Business Support IG lead.

Toolkit Requirement	Recommendation	Proposed action	Responsible officer(s)
service user records and tracing missing records	records storage area, to take appropriate action when records are unavailable and to trace missing records.	manage in particular records sent for remote storage.	
	2 All relevant staff members should be informed about the procedures, and in particular of their own responsibilities to comply with the record tracking process, and to appropriately report unavailable or missing records. Informing staff may be through team meetings, awareness sessions, staff briefings or training.	Need to ensure relevant teams have this in place, it is embedded into MIP and induction processes and as part of regular team briefing cascades.	AHH and CYP Information Asset Owners, Business Support IG lead.