Sultan
ADVISORY

Derby City Council

Information Governance Toolkit

June 2014

Background

Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information, for NHS organisations and their partners for:

- Implementation of advice and central guidance
- Compliance with the law
- Year-on-year improvement plans

Good information governance is about setting a high standard for the handling of information. The ultimate aim is to demonstrate that the Council can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

There are many different standards and legal rules that apply to information handling, including:

- The Data Protection Act 1998
- The Confidentiality NHS Code of Practice
- The NHS Care Record Guarantee for England
- The Social Care Record Guarantee for England
- The international information security standard: ISO/IEC 27002
- The Information Security NHS Code of Practice
- The Records Management NHS Code of Practice
- The Freedom of Information Act 2000

Due to the range and complexity of the standards and legal rules, the Department of Health has developed sets of information governance requirements, available in the IG Toolkit, which enable NHS and partner organisations to measure their compliance. The requirements cover all aspects of information governance including:

- Data protection and confidentiality
- Information security
- Information quality
- Care records management
- Corporate information

The purpose of this review was to assess Derby City Council's compliance with the Local Authority Version of the IG Toolkit. The Council needs to achieve, as a minimum, Level 2 compliance as part of its partnership work and Public Health responsibilities.

This is the Council's first IG Toolkit submission.

Acknowledgements

Thank you to all staff who assisted with this review. In particular, to the Head of Governance and Assurance, who was helpful in identifying key staff, locating documentation and arranging meetings. The support has been appreciated and has helped to report on the review's findings within the agreed timescales.

Key Findings

The Council's existing information governance arrangements are not mature enough for it to achieve Level 2 across all relevant sections of the Local Authority version of the IG Toolkit. It is, therefore, not regarded as a 'trusted organisation' as required by the Department of Health for information sharing purposes.

It is evident that the Council has started on improvement work in the area of information governance in the past 18 months. Examples of initiatives include:

- The establishment of the IG Board
- Drafting and approval of a number of key information governance and risk management policies
- Creation of an overall IG Action Plan, that has delivered, to date, significant progress on agreed work
- Using independent consultants to review procedures for specific areas, such as the ICO's reviews of data protection.

There remains, however, considerable work to be completed before the Council will be in a position to score itself at Level 2 or above. The following areas require particular focus in the coming months:

- Completing the substantial work required to obtain a renewal certificate for the Public Services Network. The certificate expired in June 2014 and this has had a significant impact on the scores for the IG Toolkit, as information security assurance is a key aspect of the tool;
- Defining clearly the roles and responsibilities of all Information Asset Owners so that they can take a lead role on assessing the risks relating to and protecting their information assets. Key to this work is completing the work, as agreed as part of the IG Action Plan, to create an Information Asset Register. To date, there is evidence only for AHH having completed the necessary assessments to compile and agree an asset register;
- Reviewing existing information governance policies to assess whether they remain valid and reflect the current IG framework and staff resource structures. These should be brought together by creating an overarching governance policy. This will help staff to refer to one key document with suitable appendices available for specific topics;
- Review the existing staff induction and training processes, so that clear and targeted training for IG matters is suitably embedded within them and staff are aware of key responsibilities. Following on from the recent job evaluation programme, it may be useful to consider whether revised job descriptions need to be issued;
- Review and clarify business continuity responsibilities between IAOs and the ICT department and update plans following risk assessments;
- Review existing contractual agreements with all third party suppliers and contractors to assess whether adequate IG clauses have been incorporated into agreements; and
- Review and define more clearly the Council's information quality and performance improvement protocols. In particular, update the Information Quality policy and associated procedures, working to national guidance.

IG Framework	Findings/Existing Evidence	Current Level	Recommended Action
There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda			
Requirement No. 12-144 **Required for Level 2:** The Information Governance Management Framework must be documented. The Information Governance Management Framework must be signed off by the Board or equivalent senior management tier and the key governance bodies have been established and are active. In-year reports and briefings on Information Governance arrangements are provided to the senior level of management in the organisation so that any necessary improvements to existing arrangements can be made. **For Level 3:** The senior level of management is routinely and adequately briefed on IG arrangements, any resourcing issues and considers improvements required either in-year or for the forthcoming year.	IG Board in place with documented IG Framework signed off by senior management. SIRO, IG lead and Caldicott Guardian appointed. Some examples of updates on information matters as part of the overall governance updates, e.g. for DPA, FOI going to IGB and Audit Committee. There is no resource plan for the IG activity required for the delivering the Framework nor ensuring compliance with the IG Toolkit. The current Caldicott Guardian is not on the national register.	**2**	1. Further improvement to defining governance roles, as planned, following departure of Information Governance Manager. 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. 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 contractors. 4. The Caldicott Guardian should be registered on the national register.

IG Framework	Findings/Existing Evidence	Current Level	Recommended Action
There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans			
Requirement No: 12-145 **Required for Level 2:** There are comprehensive IG policies that cover the breadth of the Information Governance agenda and have been approved by the senior level of management in the organisation. The IG policies have been communicated to staff and there are strategies and/or improvement plans in place to deliver information governance improvements, including but not necessarily limited to the IG Toolkit requirements, which have been signed off at a senior level. **For Level 3:** In year reports and briefings on the implementation of strategies and/or improvement plans are considered by the senior level of management in the organisation who also review and annually approve the IG assessment and IG improvement plan.	The following are in place: • IG Strategy and Action Plan • DPA and Confidentiality Policy • Information Security Policy • Freedom of Information Act publication strategy and procedures • IG Action Plan in place and has delivered a substantial number of agreed actions. • Records Management Policy based on Life Cycle model However, the Information Quality Policy is now deemed out of date having been last considered in 2008.	**1/2**	1. A Corporate Governance Policy should be developed 2. Develop an Information Quality policy. (An Information Quality policy is dated 2008 and no longer reflecting the current position of the Council). 3. IG Action Plan recommendations need to be updated especially around a number of key areas, such as development of the IAR. 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.

IG Framework	Findings/Existing Evidence	Current Level	Recommended Action
Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations			
Requirement No: 12-146 **Required for Level 2:** All contractors or support organisations with access to the organisation's information assets have been identified and appropriate clauses for inclusion in contracts have been developed. Appropriate clauses on compliance with IG have been put into all contracts and/or agreements. **For Level 3:** Reviews and/or audits are conducted to obtain assurance that all third parties that have access to the organisation's information assets are complying with contractual IG requirements.	Procurement policy sets out FOI and DPA clauses for tender and contract requirements for all new agreements. This applies to contracts over £30k. The procedures have been in place for the past 18 months. A template is provided for all directorates. A review of all existing contracts has not been performed to assess whether adequate IG clauses are included.	**1**	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. 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.

IG Framework	Findings/Existing Evidence	Current Level	Recommended Action
Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation.			
Requirement No: 12-147 **Required for Level 2:** All current and new employment contracts contain appropriate IG compliance requirements. An action plan has been documented to ensure that individuals working on behalf of the organisation understand their responsibilities. The action plan has been implemented and all existing staff are aware of their obligations for IG. 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. **For Level 3:** Staff awareness of their responsibilities and their compliance with IG requirements is checked and monitored.	The e-learning portal is used by staff to read IG policies. No further evidence that staff have read and understood these. There is no IG action plan for raising awareness.	**1**	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 read and adhered to. 2. The induction training and staff code of conduct should be reviewed to make that the existing processes can make sure staff are aware of the latest policies and improvements and read and understand them. 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. 4. All employment contracts should contain appropriate IG clauses.

<table>
<tr><th>IG Framework</th><th>Findings/Existing Evidence</th><th>Current Level</th><th>Recommended Action</th></tr>
<tr><td colspan="4"><b>The training needs of all staff are assessed in relation to Information Governance requirements and they are all appropriately trained</b></td></tr>
<tr><td><b>Requirement No: 12-148</b>
<b>Required for Level 2:</b>
An IG training programme has been developed that includes training needs analysis and induction for new starters.
All staff members have completed IG training. Training needs are regularly reviewed and re-evaluated when necessary.
<b>For Level 3:</b>
Action is taken to test and follow up staff understanding of IG and additional support is provided where needs are identified.</td><td>E-learning portal contains records of all training completed including a number on IG related content. It is not clear if reports from this portal can be extracted to match against each member of staff to assess whether all staff have read key policies and taken the on-line assessments, where required.
If the PSN Certificate is renewed this would be an automatic score of 2.</td><td><b>1</b></td><td>Renew PSN Certificate
OR
1. Responsibility should be assigned to an individual or team to develop the information governance training programme.
2. A training needs analysis review should be performed that highlights how existing training is meeting required IG needs.
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).</td></tr>
</table>

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed need			
Requirement No. 12-251 **Required for Level 2:** An appropriate Caldicott Guardian has been appointed and there is a documented plan in place for a Caldicott function, which has been approved by senior management or committee. There is a Caldicott function with adequate confidentiality and data protection skills, knowledge and experience to successfully co-ordinate and implement the confidentiality and data protection work programme. **For Level 3:** The confidentiality and data protection work programme is incorporated into the broader Information Governance arrangements.	A Caldicott Guardian has been appointed but there is no evidence of a defined function to support this role. Following the departure of the IG Manager, plans are in place, but have not yet been completed, to provide appropriate training to the Council's DPA and FOI leads. The Council has been audited by the ICO and an action plan is in place. This has been incorporated into the IG Action Plan.	**1**	1. All Data Protection Officers should have specialist training and appropriate qualifications. 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.

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users			
Requirement No: 12-252 There is documented guidance for staff on keeping personal information secure and on respecting the confidentiality of service users that has been approved by senior management or committee. The documented and approved staff guidance has been made available at appropriate points in the organisation and all staff members have been effectively informed about it and the need for compliance. Where appropriate the guidance is tailored to particular staff groups or work areas. **For Level 3** Staff compliance with the guidance on keeping personal information secure and on respecting the confidentiality of service users is monitored and assured.	Responsibility for ensuring staff have access to appropriate and up to date guidance on keeping personal information secure and on respecting the confidentiality of service users has been assigned to the IGB.	**1**	The Staff Code of Conduct needs to be reviewed to incorporate 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; • 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 procedures, any information sharing protocols agreed with external organisations, encryption requirements for mobile devices etc; • Who to approach within the organisation for assistance 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.

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
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 disclosure of confidential personal information are appropriately respected.			
Requirement No: 12-253 **Required for Level 2:** There are guidelines for staff on when it is both lawful and appropriate to share confidential personal information and on respecting service user wishes. The guidelines have been approved by senior management or an appropriate committee. The documented and approved guidelines have been made available at appropriate points in the organisation and all staff members have been effectively informed about the need to comply with them. **For Level 3:** Staff compliance with the guidelines is monitored to ensure, unless there is a legal reason not to, they respect service user choices when disclosing confidential personal information.	No policy available on the Intranet or staff learning sites.	Insufficient evidence to attain Level 1.	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.

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
Individuals are informed about the proposed uses of their personal information			
Requirement No: 12-254 **Required for Level 2:** General communication materials are available to inform individuals accessing services about the use of their personal information. The general communication materials are supported by an active communications campaign to inform all individuals, including those with special/different needs, about how their personal information is used. **For Level 3:** Staff compliance with their responsibilities to ensure individuals have access to the communications materials about the use of personal information is monitored and assured.	The following are in place: • Leaflets for public, staff and councillors on these issues are available. However, these need to be updated as staff referenced no longer work for the Council and the content may not reflect the current IG Framework • These materials are on the Intranet site and external website • Materials in different formats (for example, large print, Braille, audio-tape, different languages) are offered • Translation services are available There is, however, no formal communications strategy.	**1**	1. A formal communications strategy to provide more comprehensive information services to users should be established. 2. All staff members should then be effectively informed about the existence of the updated materials.

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
Where required, protocols governing the routine sharing of personal information have been agreed with other organisations.			
Requirement No: 12-255 **Required for Level 2:** A process has begun to identify and document the information requirements of each of the organisation's existing and new information sharing partners. A high-level protocol approved by senior management or committee that sets out the basic information governance principles has been agreed with each of the organisations that are unable to demonstrate the required information governance performance and with those with whom personal information is routinely shared for non-care purposes. **For Level 3:** The high level protocol is augmented by specific sections which apply to each sharing partner so that there are appropriate protocols agreed with each of the organisations that are unable to demonstrate the required information governance performance and with those with whom personal information is routinely shared for non-care purposes. Additional protocols are agreed with all new information-sharing partners.	The Council's IG Action Plan for establishing IAR requires this assessment but this work is in the early stages for all Directorates except AHH, where the data flow-mapping and IAR has been established.	**1**	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. 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). 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.

Confidentiality and Data Protection Assurance	Findings/Existing Evidence	Current Level	Recommended Action
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			
Requirement No: 12-256 **Required for Level 2:** There is a documented procedure and structured approach for ensuring that new or proposed changes to organisational processes or information assets are identified and flagged with an appropriate information governance group or equivalent and that information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project cycle. All staff members who may be responsible for introducing changes to processes or information assets have been effectively informed about the requirement to seek approval from the appropriate group. All new implementations follow the documented procedure. Where the proposed new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate privacy impact assessment is always carried. **For Level 3:** Compliance with the guidance is monitored by reviewing any new processes or information assets that have been introduced. Project assurance processes are in place and the results are fed through project boards or similar groups. Remedial or improvement action is documented and taken where appropriate.	If PSN Certificate was renewed this would be an automatic score of 2. The existing project management guidance does not contain explicit references to information governance.	Insufficient evidence to attain Level 1.	Obtain PSN certification OR 1. Update the existing project management framework so that all new projects or significant changes are required to consider information governance risks and controls.

Information Security Assurance	Evidence	Current Level	Recommended Action
The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs			
Requirement No: 12-371 **Required for Level 2:** There is an appropriately trained Information Security Manager/Officer, or access to such expertise and a documented plan in place to support Information Security Assurance, which has been approved by senior management or committee. There is an appropriate Information Security framework in place with adequate skills, knowledge and experience to successfully co-ordinate and implement the Information Security agenda. **For Level 3:** The Information Security framework is incorporated within the broader Information Governance and corporate risk management arrangements.	If PSN Certificate was renewed this would be an automatic score of 2 An Information Security Policy is in place. There is no dedicated Information Security Manager/ Officer in post.	Insufficient evidence to attain Level 1.	Renew PSN Certificate OR 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. 2. Responsibility for supporting the Information Security agenda should be identified in various staff roles co-ordinated by the Information Security Manager/Officer and includes corporate responsibility at the IGB level.

Information Security Assurance	Evidence	Current Level	Recommended Action
A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed			
Requirement No: 12-372 **Required for Level 2:** There is a formally documented Information Risk Assessment and Management Programme, which has been approved by senior management or committee. The Information Risk Assessment and Management Programme is a core activity for the organisation. **For Level 3:** The Information Risk Assessment and Management Programme is reviewed regularly and the findings appropriately reported.	If PSN Certificate was renewed this would be an automatic score of 2 There is no documented Information Risk Assessment and Management Programme - only a Risk Management Policy and this is very high level.	There is insufficient evidence to attain Level 1.	Obtain PSN certification OR 1. Document an Information Risk Assessment and Management Programme, and establish associated strategies, policies and procedures. The Programme should be approved by the IGB. 2. Update the Council's risk register with this information 3. The results of information risk assessments and recommendations should be reported to the IGB. 4. Internal audit should review the risk assessment programme on a regular basis to assess its effectiveness.

Information Security Assurance	Evidence	Current Level	Recommended Action
There are documented information security incident / event reporting and management procedures that are accessible to all staff			
Requirement No: 12-373 **Required for Level 2:** There are documented and approved processes for reporting, investigating and managing information security Incidents / events. The information security event reporting and management procedures have been communicated to staff/relevant third parties. Contracts or agreements with service providers and business partner organisations have been reviewed to ensure these include clear reporting requirements, enforceable obligations, expectations and references to procedures for the reporting of and response to incidents. **For Level 3:** The SIRO and IAOs or equivalent, monitor compliance with the procedures, taking corrective action if evidence of non-compliance is discovered. Incidents are analysed and where necessary, systems and processes are refined to minimise the risk of recurrence.	If PSN Certificate was renewed this would be an automatic score of 2 It is not clear whether there are documented procedures for reporting, investigating and managing information security events. Contracts with third parties are not reviewed to consider whether relevant security reporting clauses are in place. This review is yet to take place.	There is insufficient evidence to attain Level 1.	1. The Caldicott Guardian should ensure that she is aware of all information security incidents involving unauthorised disclosure of confidential service user information. 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. 3. The Council should ensure that responsibility for managing 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. 4. Documented reporting, investigating and managing information security events procedures need to be established. The procedures should be approved by the IGB. 5. Staff briefings on this matter should take place or inclusion of information security reporting on the e-learning portal. 6. As part of the work to review existing contracts - to be started - consider information security alongside IG requirements.

Information Security Assurance	Evidence	Current Level	Recommended Action
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			
Requirement No: 12-374 **Required for Level 2:** There are documented requirements for access controls for all key information assets. Access rights for specific individuals/groups have been agreed and documented in relation to these information assets. There are appropriate user access management procedures (including user registration, update and deregistration processes), technical functionality and management controls for all key information assets. **For Level 3** Regular reviews are carried out to audit and assure the access control and management processes. Prompt action is taken to update, replace, disable or remove profiles and individual accounts. Regular assurance reports are provided to the SIRO (or individual with equivalent responsibilities).	If PSN Certificate was renewed this would be an automatic score of 2. IAOs have not reviewed and approved access controls for the systems under their control.	There is insufficient evidence to attain Level 1.	1. Renew PSN Certificate OR 2. Responsibility for defining and documenting requirements for both system and user access controls should be assigned to IAOs. 3. IAOs should ensure that there are approved access controls in place for each key information asset under their control.

Information Security Assurance	Evidence	Current Level	Recommended Action
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			
Requirement No: 12 - 375 **Required for Level 2:** There is a documented and approved plan for securing digital and hardcopy transfers / flows of person identifiable and sensitive information in and out of the organisation. Routine transfers of person identifiable and sensitive information in all areas have been identified, mapped and risk assessed. All risks are appropriately recorded in the risk register along with the actions taken to secure the information. IAOs (or equivalent) have developed information agreements and procedures to ensure transfers are adequately protected, and ensure their staff who transfer or receive this information are effectively informed of the procedure which applies to the transfer method they use. **For Level 3:** Information risk leads (SIRO and IAOs) routinely review information transfer policy, procedures and agreements, to ensure that the measures in use continue to be effective and to consider changes to the existing procedures and alternative methods of transfer. Monitoring arrangements exist to ensure compliance and effectiveness of policy and procedures.	If PSN Certificate was renewed this would be an automatic score of 2	There is insufficient evidence to attain Level 1.	Renew Public Services Network Code of Connection Certificate. OR 1. Document a plan to ensure transfers, of person identifiable and sensitive information, to and from the Council are risk managed and adequately secure. 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. 3. Up to date information transfer agreements should be established with partner organisations.

Information Security Assurance	Evidence	Current Level	Recommended Action
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			
Requirement No: 12 - 376 **Required for Level 2:** The information risk lead (the Senior Information Risk Owner) ensures the organisation is developing its approach for ensuring recovery and continuity in the face of disaster or other major incident or business disruption. Information Asset Owners are aware of their responsibility to ensure the integrity and availability of their information assets (processing facilities, communications services and data). Approved Business Continuity Plans are in place for all critical Information Assets and all staff are aware of their roles and responsibilities. Information Asset Owners (or equivalent) have implemented approved procedures and controls for their information assets and have effectively informed all relevant staff. **For Level 3:** Business continuity plans, and system specific procedures and control measures are regularly reviewed, and where necessary tested, to assess their ability to meet their business objectives.	There is no documented business continuity strategy and associated programme.	There is insufficient evidence to attain Level 1.	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. 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. 3. The documented strategy and associated programme should appear in the relevant Information Asset Register when this has been completed. 4. IAOs should develop system level security policies that include all aspects of back up arrangements for the key assets.

Information Security Assurance	Evidence	Current Level	Recommended Action
Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.			
Requirement No: 12-377 **Required for Level 2:** Information Asset Owners (IAO) or equivalent who are responsible for key IT equipment have ensured that there are documented procedures and controls to prevent the processing of their information assets being interrupted or disrupted through equipment failure, environmental hazard or human error. The procedures and controls have been approved by the information risk lead (Senior Information Risk Owner), CIO/Head of ICT and IAO as fit for purpose. Information Asset Owners or individuals with equivalent responsibility have implemented the planned procedures and controls for their information assets. **For Level 3:** Information Asset Owners or individuals with equivalent responsibility conduct regular reviews of documented procedures and controls, monitor staff and contractor compliance and provide regular assurance reports to the Senior Information Risk Owner or equivalent.	If PSN Certificate was renewed this would be an automatic score of 2.	There is insufficient evidence to attain Level 1.	See 12-372 for further information and recommended actions.

Information Security Assurance	Evidence	Current Level	Recommended Action
Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code			
Requirement No: 12 - 378 **Required for Level 2:** All Information Assets have been reviewed to identify those which are vulnerable to malicious or mobile code and appropriate controls and procedures have been identified and documented to enable the rapid detection, isolation and removal of malicious code and unauthorised mobile code. The approved and documented controls and procedures to mitigate against malware risks have been implemented. **For Level 3:** There are routine reviews of all relevant Information Assets to ensure that implemented controls are operating according to the agreed specification. Alerts are proactively monitored and investigated.	If PSN Certificate was renewed this would be an automatic score of 2. The Council-wide IG Plan has acknowledged the need to create an IAR. This is in progress for all Directorates, except AHH, where it has been completed.	There is insufficient evidence to attain Level 1.	Renew Public Services Network Code of Connection certificate. OR 1. Document controls and procedures to mitigate against malware risks and fully implement across the Council. This includes a documented information asset register. 2. Assess whether malware solutions and controls are working through the use of system reports.

Information Security Assurance	Evidence	Current Level	Recommended Action
Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely			
Requirement No: 12-379 IAO's or equivalent responsible for ICT networks have reviewed Information Security risks. Responsibility for network security has been assigned to an IAO (or equivalent) who undertakes reviews of information security risks. Mitigating procedures, controls and responsibilities are identified and documented. The approved procedures and controls for network security in respect of all information networks controlled by the organisation have been implemented. **For Level 3** Compliance with the implemented network security controls and procedures is monitored, and remedial or improvement action is promptly taken. Regular security risk reviews and assurance reports are provided to the SIRO (or equivalent).	If PSN Certificate was renewed this would be an automatic score of 2.	There is insufficient evidence to attain Level 1.	Renew PSN Certificate OR 1. A network security policy needs to be produced for each ICT network and systems approved by the relevant IAO. 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.

Information Security Assurance	Evidence	Current Level	Recommended Action
Policy and procedures ensure that mobile computing and teleworking are secure			
Requirement No: 12 - 380 **Required for Level 2:** The IAO (or equivalent) ensures there is a documented policy for approvals and authorisation for mobile working and teleworking arrangements. The procedure is supported by documented guidelines for staff on expected NHS IG information security and confidentiality practice. All mobile or teleworkers are appropriately approved, authorised and made aware of procedures/guidelines. Robust remote access solutions and adequate information security functionality for mobile devices and removable media has been provided. **For Level 3:** There are regular reviews to audit and monitor mobile and/or teleworking arrangements and the remote working procedures and controls. Where a need for improvement or non-compliance is identified this is documented and appropriate action taken.	If PSN Certificate was renewed this would be an automatic score of 2.	Insufficient evidence to attain Level 1.	Renew PSN Certificate OR 1. Document procedures for mobile working or teleworking that provide guidelines for staff on expected behaviours. 2. Assess whether robust remote access solution(s) are in line with the PSN requirements.

Information Security Assurance	**Evidence**	**Current Level**	**Recommended Action**
There is an information asset register that includes all key information, software, hardware and services			
Requirement No: 12-381 **Required for Level 2:** Responsibility has been assigned to a staff member for compiling information about the organisation's assets and for maintaining the asset register. A list of information assets has been compiled in a register which includes the location and 'owner' for each asset. **For Level 3:** The asset register is maintained, reviewed and updated as necessary. Responsibilities and the asset register are regularly reviewed.	The Council-wide IG Plan has acknowledged the need to create an IAR. This is in progress for all Directorates, except AHH, where it has been completed.	There is insuffi-cient evidence to attain Level 1.	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.

Information Security Assurance	Evidence	Current Level	Recommended Action
All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures			
Requirement No: 12 - 382 **Required for Level 2:** There is an Information Asset Register that includes all assets that comprise or hold personal data, with a clearly identified accountable individual (IAO). All mandatory safeguards are in place to protect assets that comprise or hold personal data and risk assessments have been conducted to determine which additional safeguards should be in place. **For Level 3:** All information assets that comprise or hold personal data have been effectively secured and audit/spot checks are used to check compliance.	If PSN Certificate was renewed this would be an automatic score of 2. There is no documented Information Asset Register.	There is insufficient evidence to attain Level 1.	Renew PSN Certification OR 1. Compile local IARs using flow-mapping and IAR template completed by AHH. 2. A clear description of the safeguards that have been deployed should be included within the Information Asset Register. 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.

Information Security Assurance	Evidence	Current Level	Recommended Action
The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate			
Requirement No: 12 - 383 **Required for Level 2:** There is a clear plan for protecting the confidentiality of service user information by using appropriate pseudonymisation and anonymisation methods for purposes other than direct care. Robust information governance processes have been established to support the implementation of the pseudonymisation/anonymisation plan. **For Level 3:** Business processes are reviewed to ensure that the organisation remains compliant with the requirements to protect the confidentiality of service user information. (Requires external report)	There is no documented evidence that pseudonymisation and anonymisation techniques are being applied.	There is insufficient evidence to attain Level 1.	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).

Care Records Assurance	Evidence	Current Level	Recommended Action
The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience			
Requirement No: 12 - 441 **Required for Level 2:** There are appropriately skilled Information Quality and Records Managers/Officers in place and there are documented information quality and records management strategies and policies approved by senior management/ committee, which form part of the broader framework of information and records management policies. There is an appropriate Information Quality and Records Management framework in place with adequate skills, knowledge and experience to successfully co-ordinate and implement the information quality and records management agenda. **For Level 3:** Information Quality and Records Management arrangements are coordinated by the lead manager/officers but are incorporated within broader IG arrangements.	A Head of Quality and Performance is in post. The function sits within the Chief Executive's Office. The Data Quality Policy was drafted in 2008 and now needs updating.	**1**	1. Update Data Quality Policy. This should be approved by the IGB and issue to all relevant staff. 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. 3. Training should be provided where deemed necessary, depending upon role.

Care Records Assurance	Evidence	Current Level	Recommended Action
There is consistent and comprehensive use of the NHS Number in line with National Policy requirements			
Requirement No: 12- 442 **Required for Level 2:** There is a project plan in place to support the consistent and comprehensive use of NHS Number. The project has been successfully completed to the point where access to national systems is assured and can proceed. **For Level 3:** The NHS Number implementation programme has been successfully completed and closed and a process is in place to ensure that all new IT systems are compliant with applicable NHS Number standards and/or guidance.	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 review. If the relevant documentation is available, the score could be amended to a 2.	There is insufficient evidence to attain Level 1.	See comments left under ‘evidence’.

Care Records Assurance	Evidence	Current Level	Recommended Action
Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care			
Requirement No: 12 - 443 **Required for Level 2:** There are documented and approved procedures to ensure the accuracy of service user information on all systems and/or records that support the provision of care. Data collection and validation activities are 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. **For Level 3:** Regular audits and reviews are carried out to monitor the effectiveness of data collection and validation activities.	There are no documented procedures. There are no procedures for regular monitoring of data collection and validation.	Insufficient evidence to attain Level 1.	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. 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.

Care Records Assurance	Evidence	Current Level	Recommended Action
Procedures are in place for monitoring the availability of paper service user records and tracing missing records			
Requirement No: 12 - 444 **Required for Level 2:** There are documented and approved procedures to monitor the availability of paper service user/social care records, including tracking records and tracing missing records. The procedures for monitoring the availability of paper service user/social care records have been implemented and action taken where availability of records is considered poor. **For Level 3**: Staff compliance checks are routinely undertaken to ensure staff are following the record tracking process and appropriately reporting unavailable or missing records**.**	No documented procedures in place. However, very few paper records are maintained.	Insufficient evidence to attain Level 1.	1. Document procedures for monitoring paper service user record availability, which includes measures to track records removed from the records storage area, to take appropriate action when records are unavailable and to trace missing records. 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.

Sultan
ADVISORY

This document is private and confidential and for the use of Derby City Council only. Its contents may not be shared with third parties without permission.