TELFORD & WREKIN COUNCIL

AUDIT COMMITTEE – 15 SEPTEMBER 2015

CALDICOTT GUARDIAN ANNUAL REPORT

REPORT OF THE DIRECTOR OF HEALTH, WELLBEING & CARE/CALDICOTT GUARDIAN

LEAD CABINET MEMBER – CLLR ARNOLD ENGLAND

PART A) – SUMMARY REPORT

1. SUMMARY OF MAIN PROPOSALS

1.1 The report sets out:

- the roles and responsibilities for managing the Council's compliance with the revised Caldicott Principles (See Appendix 1) and the requirements of the Data Protection Act 1998
- an update on previously identified actions
- a plan of activity for the next 2 years

2. RECOMMENDATIONS

2.1 Audit Committee note contents of the Caldicott Guardian's Annual Report

2.2 Audit Committee receive further such reports on an annual basis commencing June 2016, with a progress update in September as part of the general Information Governance update.

3. SUMMARY IMPACT ASSESSMENT

COMMUNITY IMPACT	Do these proposals contribute to specific Co-operative Council priorities?	
	Yes	*Vulnerable Children and Adults*
	Will the proposals impact on specific groups of people?	
	No	
TARGET COMPLETION/DELIVERY DATE	*Next Annual Report to be presented to Audit Committee in June 2016 and annually thereafter*	
FINANCIAL/VALUE FOR MONEY IMPACT	Yes	There are no direct financial implications arising from the recommendations of this report. The actions set out in section 4.22 of the report will be accommodated from within existing resources and will help to ensure that the Council has appropriate arrangements in place to protect service user data. Failure to have proper arrangements in place to protect the confidentiality of service user information could result in data breaches which, if serious, could result in fines of up to £0.5m as well as causing distress to service users and their families.
LEGAL ISSUES	Yes	Each NHS organisation is required to have a Caldicott Guardian under Health Service Circular HSC 1999/012 dated 22 January 1999. The Circular applies to all organisations which have access to patient records, including acute trusts, ambulance trusts, mental health trusts, primary care trusts, strategic health authorities, and special health authorities such as NHS Direct. Caldicott Guardians were subsequently introduced into social care with effect from 1 April 2002, under Local Authority Circular LAC (2002)2 dated 31 January 2002. Caldicott Guardians play a key role in ensuring that the NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for

		handling patient identifiable information under a framework which complies with the requirements of the Data Protection Act 1998; they actively support work to enable information sharing where it is appropriate to share; and advise on options for lawful and ethical processing of information. NHS and Social Care Caldicott Guardians are required to be registered on the publicly available National Register of Caldicott Guardians. The UK Council of Caldicott Guardians, an elected body made up of Caldicott Guardians from health and social care, meets four times per year and has a published strategy, currently for 2011-2016. The Health & Social Care Information Centre [HSCIC] publishes guidance and resources for Caldicott Guardians. KF. 27.08.2015
OTHER IMPACTS, RISKS & OPPORTUNITIES	No	
IMPACT ON SPECIFIC WARDS	No	

4. INFORMATION

4.1 This Annual Report is designed to support Telford & Wrekin Council's Data Protection and Confidentiality Policy and describes how the Council can obtain assurance to address its confidentiality and data protection assurance needs (as part of good governance and as required by the Health N3 Information Governance Toolkit).

4.2 The Report sets out:

- the roles and responsibilities for managing the Council's compliance with the revised Caldicott Principles (See Appendix 1) and the requirements of the Data Protection Act 1998
- an update on previously identified actions
- a plan of activity for the next 2 years

4.3 This Caldicott Guardian (CG) Annual Report will be presented to the September 2015 meeting of the Audit Committee and annually thereafter at the June Audit Committee Meeting, with an update at the September Audit Committee Meeting

4.4 Caldicott Function – Key Responsibilities

4.5 The CG is responsible for safeguarding and governing the uses of personal care information within the Council, acting as the 'conscience' of the organisation. The CG actively supports work to facilitate and enable care information sharing and provides advice on options for lawful and ethical processing of information as required. Caldicott Guardianship is a key component of broader information governance responsibilities. The key responsibilities of the role are defined in the CG Manual (2006) as:

- **Strategy & Governance:** the CG should champion confidentiality issues at Board/management team level, should be represented at the organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

- **Confidentiality & Data Protection expertise:** the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.

- **Internal Information Processing:** the CG should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit (See Appendix 2).

- **Information Sharing:** the CG should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT systems, disclosure to research interests and disclosure to the Police.

4.6 In line with a key recommendation of the 1997 Caldicott Report, the Council has since then appointed a CG. The CG is currently the Director of Health, Wellbeing and Care.

4.7 More recently, at the request of Government, a comprehensive review was undertaken by Dame Fiona Caldicott into the original Caldicott principles. Government subsequently set out 26 recommendations some of which apply to Local Government in "*Information: To Share or not to Share – Government Response to the Caldicott Review*". At 4.21 I set out the relevant recommendations as part of a 2015/17 CG action plan.

4.8 The N3 Information Governance Toolkit (See Appendix 2) has to be completed on an annual basis. The Council's last submission for 14/15 was approved by the HSCIC on 1/4/15. However HSCIC did note some actions that require review before the 15/16 submission (to be submitted by end of March 16), as follows:

1. Requirement 146 - there is no list of contractor organisations.
2. Requirement 147 (1a) - there is no sign off for the contract clauses
3. Requirement 376 - there is no mention of the asset register.

4.9 Progress on previously identified Actions:

4.10 Research whether the comprehensive use within the authority of the unique NHS identity number (which is mandatory within the NHS and recommended elsewhere) would assist the Council in promoting and assuring information security.

4.11 A final report has been received from ICT for data-clean up, where records are missing a specific piece of information required to pull the NHS number through, e.g. actual date of birth or postcode. Business Systems Support are working through this. Following completion (by the end of September), ICT will upload the NHS matching software, match the records and run scripts to pull the NHS numbers through. We have agreed to run the NHS uploads on a quarterly basis.

4.12 Review the extent to which secure email facilities or valid alternative solutions are available to staff who need them for the communication of confidential personal information.

4.13 All officers in Social Care have at least 2 secure electronic communication methods available:

1) They can have access to a GCSX email account (subject to meeting minimum requirements for this) which will allow secure communication to other secure public sector email accounts
2) They have automatic access to the Council's Secure Communication System which allows an officer to securely communicate information to any external 3rd party.

4.14 Collaborate with Information governance colleagues in work to address data breaches, ensuring that lessons are learned and that process and practices are adjusted as necessary.

4.15 All data breaches are reported to the Information Governance Team who, in conjunction with the relevant service area, investigate the breach and ensure lessons are learnt to prevent similar incidents occurring in future. The data breach as a minimum is reported to the relevant Service Delivery Manager and possibly relevant Assistant Director dependent on the seriousness of the matter.

4.16 Further work will be undertaken to ensure enhanced collaboration is put in place between Information Governance and the CG in respect to the reporting of data breaches and the associated outcome of the incident investigation. (See 2015-17 Action Plan below)

4.17 Initiate and maintain a log of Caldicott activity and consultation.

4.18 Log initiated and maintained by Caldicott Guardian. Main areas of activity in 2014/15 were:

- Completion of training & enrolment on national register
- Sign off of data sharing agreement with Shropshire Community NHS Trust
- Information Tool Kit completion and submission
- Moving forward work to be able to use NHS number as client record identifier
- Discussion and advice with regard to information sharing with external organisations in respect of a number of individual service users

4.19 Ensure arrangements are in place to deputise for the CG in their absence.

4.20 The Assistant Director Adult Social Services (currently Richard Smith) will deputise for the CG in their absence, and undertake appropriate training.

4.21 CG Action Plan for 2015-17

4.22 The table below sets out a CG Action Plan for the next two years, taking forward the actions arising from the Caldicott Review and subsequent Government recommendations, together with other recommended actions.

Action	Target date	Lead
Caldicott Review related actions - () = Recommendations from Caldicott Review		
1. Examine our existing arrangements, and lead by example with our local partners to make it easier to share information (introduction)	Ongoing	CG
2. Ensure that relevant personal confidential data is shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual (2)	Ongoing	CG
3. Seek advice from the ICO and refer to the HSCIC's Confidentiality Code of Practice for further advice on managing and reporting data breaches (5)	As required	CG
4. Explain and apologise for every personal data breach, with appropriate action agreed to prevent recurrence (5)	As required	CG
5. Clearly explain to patients and the public how the personal information we collect could be used in de-identified form for research, audit, public health and other purposes (7)	Review public information given by March 2016	CG
6. Make clear what rights the individual has open to them, including any ability to actively dissent (7)	As per 5. above	CG
7. Use the best practice contained in the HSCIC's Confidentiality Code of Practice when reviewing information governance practices to ensure that they adhere to the required standards (12)	March 2016	CG/SIRO
8. Ensure that social care providers use the Information Governance Toolkit (12)	Embed within Procurement conditions – March 2016 Monitor through Contract compliance March 2017	CG
9. Appoint a Caldicott Guardian or Caldicott lead with access to appropriate training and support (15)	**Completed.** CG appointed and registered with Social Services CG Register. CG attended accredited CG training on 18 November 2014.	CG
10. Local authorities consider extending Caldicott Guardian arrangements to children's services (15)	**Completed.** Role across Adult & Children's services	CG
11. Strengthen leadership on information governance (15)	**Completed.** Council has now established regular meetings between CG and SIRO and supporting officers within the Council to monitor progress. CG has met separately with counterparts in Shropshire Community Trust and T&W CCG. Discussions underway with wider health and social care economy about establishing a pan-Shropshire group.	CG

12. Ensure that the information provided to inform citizens about how their information is used does not exclude disadvantaged groups (19)	As per 5. above	CG
13. Use the revised Caldicott principles in all relevant information governance material and communications (25)	As per 5. above	CG
14. Investigate, manage, report and publish personal data breaches and ensure that commissioned bodies are investigated, managed, reported and published appropriately (6)	Ongoing	CG
15. Implement appropriate arrangements in relation to information governance including the demonstration of strong leadership on information governance and adopt information governance procedures that are equivalent to those already established by healthcare providers (12)	March 2016	CG
Other actions		
16. Share annual report with Audit Committee annually in June and an annual update in September.	Completed	CG
17. Address HSCIC recommendations arising from Information Governance Toolkit submission.	March 2016 ahead of next submission	CG
18. Complete register of Information Sharing Agreements and ensure reviews are held within agreed timescales.	December 2015	CG
19. Review Use of Fax Policies	December 2015	CG
20 Ensure IG training has been undertaken by all relevant staff	March 2016	CG

5. PREVIOUS MINUTES

5.1 None

6. BACKGROUND PAPERS

6.1 Caldicott Review. www.gov.uk/government/publications/the-information-governance-review

6.2 Information: To Share or not to Share – Government Response to the Caldicott Review. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Report prepared by Paul Taylor, Director of Health, Wellbeing & Care, Telephone: 01952 381200

Appendix 1 The revised Caldicott principles

1. Justify the purpose (s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don’t use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient information

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix 2

Information Governance toolkit - Local Authority Version 13 (2015-2016)

Requirements List

Req No	Description
Information Governance Management	
13-144	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
13-145	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
13-146	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
13-147	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
13-148	The training needs of all staff are assessed in relation to Information Governance requirements and they are all appropriately trained
Confidentiality and Data Protection Assurance	
13-251	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
13-252	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users
13-253	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 disclosure of confidential personal information are appropriately respected
13-254	Individuals are informed about the proposed uses of their personal information
13-255	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
13-256	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
Information Security Assurance	
13-371	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
13-372	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
13-373	There are documented information security incident / event reporting and management procedures that are accessible to all staff
13-374	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
13-	All transfers of hardcopy and digital person identifiable and sensitive information have

375	been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers
13-376	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
13-377	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.
13-378	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
13-379	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
13-380	Policy and procedures ensure that mobile computing and teleworking are secure
13-381	There is an information asset register that includes all key information, software, hardware and services
13-382	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
13-383	The confidentiality of service user information that is not involved in the process of providing direct care is protected through use of pseudonymisation and anonymisation techniques where appropriate
Care Records Assurance	
13-441	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
13-442	There is consistent and comprehensive use of the NHS Number in line with National Policy requirements
13-443	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care
13-444	Procedures are in place for monitoring the availability of paper service user records and tracing missing records