Caldicott Guardian Policy

London Borough of Barnet

Document Control

POLICY NAME	Caldicott Guardian Policy		
Document Description	Policy detailing the role of Caldicott Guardian and process for decision making.		
Document Author 1) Team and 2) Officer and contact details	 1) Information Management Team 2) Lucy Martin, lucy.martin@barnet.gov.uk ext: 2029		
Status (Live/ Draft/ Withdrawn)	Final	**Version**	01.00
Last Review Date	New Policy	**Next Review Due Date**	Feb 2017
Approval Chain:	Head of Information Management	**Date Approved**	Jan 2016

Version Control

Version no.	Date	Author	Reason for New Version
V01.00	11-08-15	Lucy Martin	New Policy

Contents

1. Introduction

The Caldicott Report: A review was commissioned in 1997 by the Chief Medical Officer of England "owing to increasing concern about the ways in which patient information is being used in the NHS in England and Wales and the need to ensure that confidentiality is not undermined. Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively".[1]

A committee was established under the chairmanship of Dame Fiona Caldicott, Principal of Somerville College, Oxford, and previously President of the Royal College of Psychiatrists. Its findings were published in December 1997.

In addition, in 2002 the Department of Health issued a Local Authority Circular (HSC 2002/003: LAC(2002)2 entitled “Implementing the Caldicott Standard into Social Care” which outlined the implementation requirements needed for all Councils with Social Services Responsibilities (CSSRs).

The 1997 Caldicott Report and the subsequent Caldicott Information Governance Review published in 2013 introduced and defined the Caldicott principles and created the role of the Caldicott Guardian, a role tasked with responsibility for appropriate use of social care related personal identifiable information.

2. Purpose and Scope

This policy provides an overview of the responsibilities of the named Caldicott Guardians. It further provides all employees, staff members or partner organisations (suppliers and contractors) with an understanding of their responsibilities in ensuring that Caldicott Guardian views and sign off are appropriately sought as and when required.

The policy applies to all “**Personal Confidential Data”** processed, stored, used or accessed in any format held by or on behalf of the council. The term used in the Caldicott Review encompasses all personal information about identified or identifiable individuals, which should be kept private or secret and includes deceased as well as living individuals.

The review interpreted 'personal' as including the Data Protection Act 1998 definition of personal data, but included data relating to the deceased as well as living people, and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

This term “personal confidential data” will be used throughout this policy.

---

1 1 The Caldicott Committee (December 1997). "The Caldicott Report". Department of Health.

All officers and individuals handling personal confidential data on behalf of the council have a personal responsibility to engage the relevant council Caldicott Guardian, and seek views opinions and sign off as and when required. Section 5 explains when an officer should involve the Caldicott Guardian.

3. Caldicott Guardian principles

The Caldicott Guardian role is mainly prominent in health organisations but is also relevant and necessary for local authorities who undertake social care responsibilities. The Caldicott Guardian plays a key role in ensuring that the organisation satisfies the highest practical standards for handling personal confidential data in a social care setting. The Caldicott Guardian acts as the 'conscience' of an organisation.

The Caldicott principles and processes provide a framework of quality standards for the management of confidentiality and access to personal information under the leadership of a Caldicott Guardian.

The primary aim of the principles is to ensure that the processing, security and confidentiality of personal information are at the forefront of information sharing.

- **Principle 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.

- **Principle 2 - Don't use personal confidential data unless it is absolutely necessary**

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

- **Principle 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 is transferred or accessible as is necessary for a given function to be carried out.

- **Principle 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.

- **Principle 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 are made fully aware of their responsibilities and obligations to respect service user confidentiality.

- **Principle 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.

- **Principle 7 - The duty to share information can be as important as the duty to protect an individual's confidentiality**

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

3.1. Caldicott Principles and the Data Protection Act

The Caldicott principles have close links to the key principles of the **Data Protection Act 1998** (which are referenced in the council's DP Policy).

There is direct correlation with a number of the principles. The more obvious ones are outlined below.

A full list of the Data Protection Principles is shown in Appendix B.

Caldicott Principles	Data Protection Act Principles
Principle 1 – Justify the purpose(s)	Principle 1 – Fair and lawful processing Principle 6 – in line with the rights of the data subject
Principle 2 – only use personal confidential data when absolutely necessary	Principle 3 – adequate, relevant and not excessive
Principle 3 – use the minimum that is required	Principle 3 – adequate, relevant and not excessive

Caldicott Principles	Data Protection Act Principles
Principle 4 – Access should be restricted on a need-to-know basis	Principle 3 – adequate, relevant and not excessive Principle 7 – kept secure
Principle 5 – Everyone must understand his or her responsibilities	Principle 7 – kept secure
Principle 6 – Understand and comply with the law	Principle 1 – Fair and lawful processing Principle 2 – used for specified and lawful purpose
Principle 7 - The duty to share information can be as important as the duty to protect an individual's confidentiality	N/A

4. Roles and responsibilities

The council has three nominated Caldicott Guardians. One is placed within the Adults and Communities delivery unit, one is within the Family Services delivery unit and an additional role is held by the council's Data Protection Officer.

At the council a number of the traditional Caldicott Guardian responsibilities are covered by the Information Management Team and the council's suite of information management policies. Therefore the Caldicott Guardian must ensure they have oversight of the policy suite, take responsibility for raising risks or issues with local (delivery unit) practices, have oversight of security incidents and information sharing affecting social care related personal confidential data and take Guardian decisions on a case by case basis as required.

Caldicott Guardians are responsible for the promotion of appropriate and lawful sharing between professionals. Encouraging officers and giving them the confidence to share personal confidential data within the framework of the principles.

The Caldicott Guardian also has a strategic role, which involves representing and championing information management at management team level and, where appropriate, at a range of levels within the council's overall governance framework. They are required to maintain close links to their delivery unit's Information Management Governance Group (IMGG) and the council's Security Forum; ensuring they report back any concerns, issues or recent decisions taken as and when they occur.

A role profile for LBB Caldicott Guardians is at Appendix A.

All officers and individuals handling data on behalf of the council have a personal responsibility to engage the relevant council Caldicott Guardian, and seek views opinions and sign off as and when required.

5. When to involve the Caldicott Guardian

The Caldicott Guardian's views must be sought ahead of:

- any new information sharing arrangement involving social care personal confidential data;
- any new project that involves the use of social care personal confidential data;
- any new system implementation and its access requirements, or any system access changes which involves the access to social care personal confidential data.

Note:

The level of involvement required by the Caldicott Guardian may differ depending on the sensitivity, volume or use of the data involved.

All Officers - It is the responsibility of the officer leading on the sharing arrangement or project to ensure that the Caldicott Guardian has been engaged at the start of the process.

Caldicott Guardian - It is the responsibility of the Caldicott Guardian to determine their level of involvement, ensuring it is sufficient enough to make an informed decision. This could be as extensive as attending frequent project meetings, or as minimal as signing off a routine Information Sharing Agreement through attendance at IMGG.

6. Decision making process

The Caldicott Guardian is seen as the conscience of the organisation (similar to the role of the Data Protection Officer) with their primary concern being that of appropriate management of personal confidential data. They should be a focal point for information sharing concerns or issues.

They act as a decision maker and are solely responsible for the decisions they make. However, it is important that the Caldicott Guardian does not make any decisions in isolation. They must ensure the views and opinions of all relevant parties are taken into account when making their decision.

The Caldicott Guardian is required to not only take into account the principles developed in the Caldicott report, but also take account of any relevant codes of conduct provided by professional bodies or guidance issued on the protection or use of personal confidential data. They must also maintain a heightened awareness of all council information management policies and ensure adherence to these when making their decision.

6.1. Register of decisions

Each decision taken by a Caldicott Guardian must be logged on the central register held by the Information Management Team (IMT). This should be used as a clear audit trail for decisions as well as a learning tool for subsequent similar requests.

The register includes:

- the date the request was passed to the Caldicott Guardian
- the person making the request
- a brief description of the matter – be careful not to include specific names of data subjects where possible
- the date the decision was made and by whom
- a justification for the decision against each principle

N.B. There is no requirement for Information Sharing Agreement (ISA) sign offs to be logged on the Caldicott register, where they have already been subject to review at IMGG.

As all Caldicott Guardians are required to attend IMGG, the Caldicott sign off for every ISA is already mandatory. ISAs are logged separately on a central ISA Register.

7. How the Caldicott Guardian & Senior Information Risk Owner work together

There are a number of distinct differences between the role of Caldicott Guardian and that of Senior Information Risk Owner (SIRO) and for that reason they remain very separate roles.

Where the Caldicott Guardian is primarily focused on personal confidential data, the SIRO concerns are much wider, with that of risks to information management more generally. The SIRO role is to understand how the strategic business goals of the organisation may be impacted by any information risks.

As part of the risk management process, information assets need to clearly be identified and "ownership" for each asset assigned to an Information Asset Owner (IAO). The SIRO is responsible for appointing IAOs to ‘own’ information assets.

The Caldicott Guardian:

- is advisory and accountable for that advice
- is the conscience of the organisation
- provides a focal point for service user confidentiality & information sharing issues
- is concerned with the management of service user information.

The Senior Information Risk Owner:

- is accountable for information risk management processes in the organisation
- fosters a culture for protecting and using data
- provides a focal point for managing information risks and incidents
- is concerned with the management of all information assets.

Despite the clear difference in roles there is a need for both roles to work together and consult where appropriate when information risks are reviewed which concern or involve the processing of personal confidential data.

8. Associated legislation and other guidance

- Data Protection Act 1998
- Human Rights Act 1998

Guidance:

- Confidentiality: NHS Code of Practice
- General Social Care Council: Code of Practice for Social Care Workers and Code of Practice for Employers of Social Care Workers 2002
- Supporting documentation located on the Health & Social Care Information Centre website - http://systems.hscic.gov.uk/infogov/caldicott/caldresources

9. Training

Each of the council's Caldicott Guardians must have undertaken specific training relevant to this role.

As a minimum each Guardian must have completed the Caldicott Guardian module entitled "The Role of the Caldicott Guardian: NHS and Social Care - Practitioner" contained within the NHS Information Governance Training Tool.

This is a practitioner level module aimed at newly appointed Caldicott Guardians, or those wanting a refresher.

IMT will also run refresher workshop sessions with all Caldicott Guardians as and when required to allow group sharing and learning on recent decisions.

All Guardians are required to register by completing the certification form on the Department of Health website and posting it to the stated address.

10. Policy review

This policy will be reviewed on an annual basis or sooner as is required where there are changes in legislation, or recommended changes to improve best practice.

11. Associated policies

This policy forms part of a suite of Information Management policies which are all available on the intranet. The policies provide further guidance on council information standards, data security and working practices which must be adhered to.

Further advice and guidance for staff is available from the Information Management Team.

Address: Information Management Team
London Borough of Barnet
Building 2, North London Business Park
Oakleigh Road South
London
N11 1NP

Email: data.protection@barnet.gov.uk

12. Appendix A – Role of the Caldicott Guardian

The role of the Caldicott Guardian is to:

- register as Caldicott Guardian on the National Register of Caldicott Guardians and ensure registration is kept up to date.
- lead and help foster a culture that values, protects and uses information for the public good.
- take visible steps to support and participate in information asset management, including participating in training.
- recognise and embrace their role as ‘conscience’ of the council in relation to personal confidential data.
- assure themselves that the council’s policies and processes governing the processing of personal confidential data in a social care setting are appropriate and proportionate.
- liaise with the IAOs for assets containing social care related personal confidential data and ensure compliance with council policies.
- consider the balance of appropriate data sharing and transparency, and confidentiality.
- have oversight of Information Sharing Agreements (ISAs) covering social care related personal confidential data.
- attend the relevant Information Management Governance Group (IMGG).
- receive reports on security or data protection incidents relating to social care related personal confidential data and make recommendations if appropriate.
- report concerns and issues in relation to incidents with the security and processing of social care related personal confidential data to IMT and the SIRO, in line with the council’s Security and Data Protection Incident Management Policy.
- report any risk issues to the Security Forum using the information security risk assessment template.
- be available to advise officers on the use of personal confidential data in a social care setting, in line with council policies.

13. Appendix B – Data Protection Act 1998 Principles

All of the eight principles must be complied with when processing / using personal data in any way: -

- **Principle One** - Personal data shall be processed *fairly and lawfully* and, in particular, shall not be processed unless: -

  (a) at least one of the conditions in Schedule 2 (of the DPA) is met, and

  (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (of the Data Protection Act) is also met.

  Additional explanation regarding this principle can be found in the Data Protection Toolkit.

- **Principle Two** - Personal data shall be collected only for one or more specified purpose, and shall not then be further used in any manner incompatible with that original purpose.

- **Principle Three** - Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) it was collected for.

- **Principle Four** - Personal data shall be accurate and, where necessary, kept up to date.

- **Principle Five** - Personal data shall not be kept for longer than is necessary for that purpose it was collected.

- **Principle Six** - Personal data shall be processed in accordance with the rights of data subjects as specified in the DPA.

- **Principle Seven** - Personal data will be kept secure at all times. Appropriate technical and organisational measures shall be put in place to mitigate against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- **Principle Eight** - Personal data shall not be transferred to countries outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.