Adult Social Care and Health Standard Operating Procedure

For the

Caldicott Guardian Function

Document Owner	Richard Smith – Corporate Director for Adult Social Care and Health
Version	V3
Revision date	April 2021

Contents

1. Introduction

A Caldicott Guardian (CG) is a Senior Manager who is accountable to the Information Commissioners Office (ICO) and the Department of Health and Social Care (DHSC) for the confidentiality and protection of Patient Identifiable Data (personal data and sensitive personal data) within their organisation. This mandatory role ensures that KCC's services and partner agencies satisfy the highest practicable handling standards of personal data and sensitive personal data.

The CG must ensure that the following principles (summary) are applied to the handling of personal data and sensitive personal data.

Principle 1: Justify the purpose(s) for using confidential information Every proposed use or transfer of confidential information should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.

2. Scope

This procedure applies to:

- Richard Smith as the accountable Caldicott Guardian
- The assigned Caldicott Guardian Support Officer Group (CGSOG) of Adult Social Care and Health (ASCH).

- ASCH and Education and Young People Managers[1] who manage or supervise the handling of Confidential Identifiable Information.
- The procedure interfaces with all KCC Information Governance policies and procedures.

3. Overview

This document sets out a mandatory procedure to support the Caldicott Guardian for the ASCH Directorate.

3.1. Richard Smith is the accountable Caldicott Guardian for Kent County Council.

3.2. The Caldicott Guardian Support Officers Group (CGSOG) is a role assigned to designated officers by the Caldicott Guardian and authorised to act on his behalf in all Caldicott Guardian related matters. The CGSOG is the single point of contact and support to ASCH Managers and Team Leaders and is responsible for ensuring compliance with the Caldicott Principles, reporting exceptions and issues to the CG as they arise.

3.3. ASCH Managers and Team Leaders are responsible for ensuring that confidential information confidential information within their services and/or teams is appropriately handled and protected, and for ensuring that the Caldicott Principles are being applied.

---

1 *For the purpose of this SOP Managers refers to all managers, whether team managers, service managers, senior practitioner, or other named management roles.*

4. Caldicott Guardian (CG)

The Caldicott Guardian:

4.1. Provides an annual Caldicott Assurance Statement to the Corporate Information Governance Group/Corporate Management Team.

4.2. Reports incidents of loss or disclosure of personal data and sensitive personal data, or breach of confidentiality to the ICO and the DHSC, and is responsible for notifying the service user/client (Data Subject) within a reasonable time should their data or consent be compromised.

5. Responds to exceptions and issues escalated or raised by the CGSOG, and where appropriate, alerts the Data Protection Officer and Senior Information Risk Owner of heightened or exceptional risk as appropriate.

6. Caldicott Guardian Support Officers Group (CGSOG)

Each relevant division has an appointed CSGOG listed in appendix 1

The CGSOG is collectively responsible for:

6.1. Providing a single point of contact to ASCH and Children, Young People and Education (CYPE) Managers regarding compliance and good practice and provides an escalation route for Caldicott related issues and concerns or where legal advice may need to be accessed.

6.2. Maintaining a log of Caldicott related events and ensuring that incidents of loss or disclosure of confidential information, or breach of confidentiality are immediately reported to the Caldicott Guardian.

6.3. Performing (or commissioning) periodic audits of Caldicott practice within ASCH and CYPE.

6.4. Receiving and responding to email alerts from the ICT Project Management Office when new information systems that process confidential information confidential information are considered, or where changes are made to existing information systems processing personal data and sensitive personal data.

6.5. Ensuring that new Information Sharing Agreements that include confidential information comply with Caldicott Principles and that the parties are signatories to the Kent and Medway Information Sharing Agreement.

6.6. Ensuring that all regular outbound confidential information flows have been identified and mapped.

6.7. Ensuring that all regular inbound flows of confidential information are recognised and handled appropriately and that ‘Safe Havens’ have been provided for receiving confidential information.

Confidential information:

6.8. Ensuring that changes to existing Information Sharing arrangements that include confidential information comply with the Caldicott Principles.

6.9. Attending quarterly meetings of the CSGOG and annual meeting with the Caldicott Guardian (see terms of reference Appendix 2).

6.10. Maintaining Privacy Notices and a record of the Privacy Notices for their Directorate/Division (as appropriate to their role).

7. ASCH and CYPE Managers

ASCH Managers are responsible for ensuring:

7.1. Those employees handling confidential information recognise and know how to handle it appropriately, and are aware of their responsibilities for confidentiality.

7.2. The RESTRICTED protective marking (SENSITIVITY LABLES) is used on all physical and digital documents and emails containing confidential information (See Protective Marking Policy and guidance).

7.3. Confidential information is transmitted, sent or received in a secure and prescribed manner that has been competently risk-assessed.

7.4. Prior approval of the Caldicott Guardian (or Deputy Caldicott Guardian in his absence) has been obtained before any new project or process involving the sharing, processing, transmission or handling of confidential information is initiated.

7.5. Compliance with the General Data Protection Regulations 2016 with regard to the sharing of Sensitive Personal Information, including personal data and sensitive personal data, with Data Processors, external agencies or other organisations.

Confidential information:

7.6. ASCH and CYPE managers must ensure that existing manual or digital information systems that process, transmit or handle confidential information are notified to the Corporate Records Manager so they can be flagged on the Corporate Information Asset Database (CIAR).

7.7. ASCH and CYPE Managers are responsible for ensuring that each confidential information item is justified and essential for the stated purpose.

8. Information, Advice and Guidance

8.1. Documents and guidance relating to the Caldicott Principles and function can be found on the ASCH Information Governance Pages.

8.2. IG documents and guidance can be found on the KNET Information Governance site, or in the Management Guide to Information Governance, also on KNE.

8.3. Advice on Information Assurance can be obtained by contacting the Information Resilience and Transparency Team: email dataprotection@kent.gov.uk

8.4. Advice on Information Security and Information Risk can be obtained by contacting the ICT Compliance and Risk Team by email: james.church@kent.gov.uk

8.5. Advice on Records Management can be obtained by contacting the Records Manager by email elizabeth.barber@kent.gov.uk.

Appendix 1

Caldicott Guardian Support Officers Group Members

- **Janice Grant,** Caldicott Guardian Support Oficer, Adult Social Care & Health
- **Matt Chatfield,** Head of Systems and Performance, Business Delivery Unit
- **Lauren Liddell-Young**, Information Governance Lead**,** Systems and Performance
- **Mark Chambers**, Head of Health Intelligence, Public Health
- **Katherine Atkinson,** Assistant Director, Management Information & Intelligence, Children, Young People and Education.
- **Kelly Leeson**, Information Governance Lead, Integrated Children's Services
- **Michael Thomas-Sam** Strategic Business Adviser Social Care, Strategy, Policy, Relationships and Corporate Assurance
- **Sandra Town**, Information Governance Specialist, Information Resilience and Transparency Team

Appendix 2

TERMS OF REFERENCE v3	
Caldicott Support Officers Group – ASCH and CYPE Directorates	
Purpose / Role of the Group	The purpose of the Caldicott Support Officers Group is to support the Caldicott Guardian in the discharge of the Caldicott function. The Caldicott Guardian is responsible for protecting the confidentiality of [patient and] service user information and to enable appropriate information sharing. The group will: • Act as the conscience of the Directorate • Support work to ensure appropriate information sharing • Advise on options for lawful and ethical processing of information And will ensure the following principles are applied in the sharing of Personal Data: • **Principle 1**: Justify the purpose(s) for using confidential information • **Principle 2**: Use confidential information only when it is necessary . • **Principle 3:** Use the minimum necessary confidential information • **Principle 4:** Access to confidential information should be on a strict need-to-know basis • **Principle 5:** Everyone with access to confidential information should be aware of their responsibilities • **Principle 6**: Comply with the law • **Principle 7:** The duty to share information for individual care is as important as the duty to protect patient confidentiality • **Principle 8:** Inform patients and service users about how their confidential information is used.
Membership	Membership of the Support Officers Group includes: • Janice Grant • Matt Chatfield • Lauren Liddell-Young • Mark Chambers • Katherine Atkinson • Kelly Leeson • Michael Thomas-Sam • Sandra Town Further details for each member listed above can be found in Appendix 1. The chair will rotate on a quarterly basis. **QUORUM** - Representation from ASCH, CYPE, Public Health,

Accountability	The Group will report to: Richard Smith, Caldicott Guardian and the Corporate Information Governance Group annually as directed.
Working Methods	**FREQUENCY OF MEETINGS** The Group will meet quarterly to: • Resolve issues raised in relation to Standard Operating Procedures developed within the directorate. • Resolve issues raised in relation to DPIAs submitted for projects under the PMO. • Review any data breaches which meet the definition of Serious Incidents Requiring Investigation. • Consider incidents to identify common themes which may inform future projects and activity within the Divisions. • Discuss and ensure implementation of relevant actions from the IGCDWG. • Develop a Caldicott function action plan as necessary.

ADVISORY NOTE:
There are considerable differences in the role between the SIRO and the Caldicott Guardian, and these are summarised in the table below. There is some overlap between the roles, particularly in developing the right organisational culture for protecting personal information.

Caldicott	SIRO
Is advisory	Is accountable
Is the conscience of the organisation	Fosters a culture for protecting and using data
Provides a focal point for patient or client confidentiality and information sharing issues	Providing a focal point for managing information risks and incidents
Is concerned with the management of patient or client information	Is concerned with the management of all information assets