CHESHIRE EAST SAFEGUARDING ADULTS BOARD

KEY SAFE PROTOCOL

Version:	2
Date Implemented:	Jan 2024
Review Date:	Jan 2026

Introduction

With more people receiving health and social care within their own homes it is important that they are protected. Cheshire East Safeguarding Board identified a need to develop a Key Safe Protocol following a recent incident, which highlighted the need to improve the way in which information on key safes is shared. The purpose of the document is to therefore set out the expectations of the Board to ensure that residents privacy and safety is not jeopardised.

What is a Key Safe?

A key safe is a small, secure box with a keypad, designed to hold keys, mounted on an outside wall. The key safe box opens when a pre-set code is entered to all access to the key(s) stored inside.

Key safes are a means of providing access to a service user's home for services such as social, nursing or medical care, by authorised providers. Most key safes have been introduced to support a care package or due to the increased needs and/or reduced mobility of the services users, to enable them to live safety within their own home.

Whilst this allows the service user to remain relatively independent within their own home, it does mean that the service user does not have control over who enters their home. Therefore care must be taken not to share the key safe code numbers with any unauthorised persons, to ensure the safety of the service user in their own home.

Cheshire East Safeguarding Boards Expectations:

Cheshire East Safeguarding Board expects all organisations who are providing health and social care within individuals own homes to respect and protect their dignity and safety. This protocol has been introduced to assist professionals to do this and to ensure that key safe numbers can be safely and efficiently shared to best support adults living in their own homes.

The expectation is that all organisations will adhere to the Caldicott Principles and will meet the requirements within the Data Protection Act as outlined within this protocol.

This will require all organisations to:

Have a Policy and clear procedures in place which will demonstrate how the Caldicott Principles and Data Protection Act, are being compiled with in relation to the use of Key Safes. Reference should be made to local information sharing protocols

The Policy and procedures should include the following but are not exclusive:

- Policies and Procedures must be clear that Key safes are to be accessed for the benefit of the service user only and that the property should only be accessed to carry out the care and support plan.

- Define clearly who would have access to the key safe.

- Outline the safe storage and use of confidential information about service users.

- Responsibility for keeping key safe codes safe and secure. Staff should be clear about their responsibilities regarding security and wellbeing.

- Where staff/volunteers fail to follow the organisations policy and procedures on information security and communication it must be clear what disciplinary action may be taken.

- It should be clear what is required of staff in a case of an emergency and who they are able to disclose the key safe code to. In the event of case of disclosure it must be clear what the process to advise service user and when a code should be changed. In the event of a life threatening emergency this could include sharing the key safe code appropriately with another Organisation or individual. Organisations must keep the service users safety paramount at all times.

- In the event of a breach of information security, all staff/volunteers must comply with their organisations reporting processes, which must be outlined within the Policy and procedures .

- Keep and maintain adequate records, including who has been given each individual key safe code, for what purpose and when.

What is Caldicott?

The term Caldicott refers to a review commissioned by the Chief Medical Officer. A review committee, under the chairmanship of Dame Fiona Caldicott, investigated ways in which patient information is used in the NHS.

The review committee also made a number of recommendations aimed at improving the way the NHS handles and protects patient information. In 2000, the government decided that these standards should be extended to "*Councils with Social Service Responsibilities",*

These are summarised by six Information Management Principles:

1) Justify the purpose for which the information is needed.

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) Only use personally identifiable information when 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 patients to be identified should be considered at each stage of satisfying the purpose(s).

3) Use the minimum personal identifiable information possible – if possible use an identifier number rather than a name.

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.

4)Access to the information 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 should be aware of his/her responsibilities to respect clients confidentiality.

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) Understand and comply with the law.

The most relevant legislation is the Data protection Act 1998, the Police & Criminal Evidence Act 1984 and the Human Rights Act 1998.

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.

Data Protection

There are 8 Principles which must be applied when handling or processing information.

Data Protection Principles

These Principles form the backbone to the Data Protection Act.

1) Information must be processed fairly & lawfully.

2) Information must be processed for the specific purpose or purposes given.

3) The information being processed is adequate, relevant and not excessive.

4) That information is accurate.

5) Information must be kept no longer than is necessary.

6) Information is processed in accordance with the subject's rights.

7) Information is kept secure at all times

8) Information is not transferred to countries or territories outside the EEA or to countries or territories without adequate protection unless Safe harbour or similar agreements are in place and in operation.