Access to Service Users' Homes for Telecare Response

Good Practice Guide

jit joint improvement team

Scottish Centre for Telehealth & Telecare

tsa telecare services association

ACKNOWLEDGEMENTS

This Good Practice Guide has been written with the purpose of sharing existing operational practice with a view to promoting improved standards of telecare service delivery across Scotland.

We would like to thank the following contributors to the writing of the guide:

Pamela Dimberline, Stirling Council

Sharon Ewen, Bield Response 24

Donna Fleming, Edinburgh City Council

Maureen Holmes – Telecare Service Association

Patrick Langan, Hanover Telecare

Mairi McIvor, Highland Council / NHS Highland

Stuart Wheeler - The Key Safe Company

Ann Steele, East Renfrewshire Council

Doreen Watson, Joint Improvement Team

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

Scotland is one of the few countries in the world with a single, unified approach to telehealth and telecare. The **National Telehealth and Telecare Delivery Plan for Scotland to 2015** was developed with partners from health, social care, housing, the third and the independent sectors to provide continued strategic direction for the use of technology to enable care in Scotland.

Workstream 6 of the Delivery Plan refers to the following action: *review potential for good practice guidelines in: Home Access for care, support and emergency services.* This document responds to that action.

A growing number of vulnerable and socially isolated people are being supported to live independently in their own homes with support packages that include home care services, community nursing and technology based services such as telehealth and telecare.

To ensure that care, support and emergency services operate with appropriate governance it is essential that procedures to access a person's home are clearly defined. These procedures should be in place in order to protect the person's health, privacy and the physical security of their home and should be agreed with the user, or their family, next of kin, representative or advocate. It is important that these procedures also provide appropriate protection for visiting staff, managers and service commissioners.

This document sets out good practice to improve service delivery in the implementation of care, support and emergency response services associated with the delivery of telehealth and telecare services.

1.2 Purpose of Good Practice Guide

The purpose of the Good Practice Guide (GPG) is to outline the best practice for access to service users homes in line with the National Care Standards http://www.nationalcarestandards.org/files/care-at-home.pdf (*note: these are currently under review*) in ensuring the security and safety of the home and service user at all times, and also the relevant legislation in relation to the processing and handling of personal information.

The Scottish Centre for Telehealth and Telecare (SCTT), the Joint Improvement Team (JIT), and the Telecare Services Association (TSA) have co-authored this Good Practice Guide which covers:

- Access by the telecare service user (tenant/owner)
- Access by a nominated key holder/volunteer responder
- Access by means of a key safe
- Access using keys held by organisations
- Remote access
- Remote access by an alarm receiving centre
- Door entry/access control systems
- Barrier free access
- Access by forced entry (by emergency services) /emergency access

2 DEFINITIONS AND ROLES

2.1 Alarm Receiving Centre / Monitoring Centre

Community alarm and telecare services require an Alarm Receiving / Monitoring Centre capable of receiving and responding to alerts raised by the equipment in order to initiate the appropriate action. Many areas have established a 24 hour call monitoring centre to perform this function, where one or more trained operators (call handlers) provide an immediate, skilled, sensitive response to the person, or to the alarm. This part of the service is referred to as an Alarm Receiving Centre (ARC), monitoring centre, or call handling service.

Detailed call handling protocols provide a series of instructions the call handler must follow in response to different situations. The call monitoring system instantly recognises the source of the alert, and core information (such as address, name of key holders, communication, support needs, essential medical information etc.) will appear on screen at the same time as the call is answered. The call handler within the ARC manages the call from the service user and uses the agreed response protocol to summon assistance. The exact nature of the response depends upon the service user's wishes and the responder services available locally.

2.2 Mobile Responder Teams

There is variation in how mobile responder services are provided across Scotland. Some areas employ teams of specially trained staff to provide the main response service to most emergency calls. Other areas use wardens, or similar staff, who can provide practical help in an emergency, and can appraise a situation (such as a fall, or failure to answer the door) so ensuring that the appropriate service is called.

2.3 Key holder

A person or organisation that holds keys to access a property. Each person or organisation should be made aware of their responsibilities around the safe keeping and use of keys (refer to Section xx - Access Using Keys Held By An Organisation), but it is not essential that they will be the first port of call when there is a need for a response following an alarm call.

2.4 Volunteer responder

A person identified by the service user who may be asked to visit the property and is willing to do so in response to alarm activation. They are generally people known to the service user who are willing to provide assistance and support. The safety and wellbeing of the service user is dependent upon the reliability, availability and capacity of the people volunteering to be responders. It is imperative that responders have this capacity in terms of physical health, and availability day and night and are aware of their responsibilities as volunteer responders. It would be good practice to specify response times within local protocols and procedures. The Telecare Services Association guidelines recommend a 45 minute maximum response time for organisations that provide their own response service.

3. LEVELS OF ACCESS

3.1 Introduction

Access to the person's home can present challenges for visiting health and social care staff, but particularly so in emergency situations. ARCs should ensure, where possible, that all service users' homes have a means of access in case of emergency. This could be via a reliable nominated 'Key Holder' who will arrive promptly, a key safe installed at the property and the access code registered with the ARC or, in some instances, keys are held by mobile responder teams.

When a service user is first assessed for a telecare service, the service user is asked to name one or more 'key holders' so that, if they are unable to answer their door when in difficulty, one of their keyholders can. The nominated key-holder is often an informal carer (any person, such as a family member, friend or neighbour who provides support or on-going assistance to another person without payment for the care given). Informal carers often play a critical role in providing a response in an emergency or enabling access for responder services.

3.2 Levels of Access

Good practice when setting up a procedure would be to manage access to service users' homes with the objective of determining exactly what level of access is required for each service provided to the user. The table below outlines suggested access levels categories.

Table 1 Suggested Access Levels Categories
(Telecare Services Associations)

Access Level	Type of Access	Description
1	Normal	Access is only given by the service user. Permission to enter the home is granted or denied by the service user at the time of the visit. Keys are not held or used by the service provider. If the service user does not reply, access is denied. Note: this is the same level of access as any general visitor to any home. Service examples: Administrative or casual visits
2	Reactive	Permission has been granted by the service user for the service provider to enter the premises if an alarm call is received. Service examples: Emergency/alarm response Note: access may be needed to deal with unconfirmed emergency calls, when no reply is received for the service user after they have initiated an alarm call.
3	Proactive	Permission has been granted by the service user for the service provider to enter the premises even when no direct request for assistance has been received. Service examples: Proactive morning check call and evening tuck-in services, home care supports etc.

4. ACCESS IS CONTROLLED BY THE SERVICE USER

4.1 Introduction

This is the simplest and most common method of entering a person's home. It can only be used to provide services to those who are mobile, able and willing to engage with services that are not considered life dependent. Examples include a community care assessment or telecare routine / check / maintenance visit.

4.2 Good practice guidance

The procedure for visiting a person at home where they are able to answer their door should be clear and the following basic rules should be followed:-

- Routine appointments where appropriate should be pre-arranged by the preferred method of communicating for the person i.e. telephone, e-mail or letter. Staff should not arrive unannounced at a person's door and expect to gain entry.
- Suitable days and times of routine visits need to be considered.
- Once at the person's door, consideration should be given to how long services should spend trying to get the person's attention. Services should follow their own internal guidelines.
- Staff should stand a reasonable distance from the door and not look through the person's windows as this can be upsetting or appear intimidating.
- Once the door has been opened, an identity card must always be shown and then a brief introduction and explanation of the purpose for the visit.
- Permission to enter the home is then granted or denied by the person at the time of the visit.

Where access by the person is not possible because of their health, mobility difficulties or where a service requires entry because of a need for assistance in an emergency, other access methods need to be considered.

5. ACCESS BY A NOMINATED KEY HOLDER AND/OR VOLUNTEER RESPONDER

5.1 Good practice guidance

The following good practice guidance is offered in relation to volunteer responders:

- The name, address and contact telephone numbers of volunteer responders should be held securely in the ARCs computer records. The information provided is subject to the provision of the Data Protection Act 1998 and should be held confidentially, and retained for processing and meeting statutory obligations.
- Nominated key holders/volunteer responders should be advised to notify the telecare service provider of any changes in their contact details or their ability to act as a nominated key holder.
- The telecare service provider should review key holders' contact details and check the suitability of key/s at service reviews, at least on an annual basis.
- The nominated key holder/volunteer responder should ensure that they have a key to the service user's home PRIOR to installation of telecare equipment.
- In the event of an activation of any telecare sensors the nominated key holder/volunteer responder may be asked to call on the service user to allow access to the property or to determine what action is required and to contact the appropriate Emergency Services for assistance if necessary.
- If the ARC triages the call immediately to the Emergency Services the key holder and/or volunteer responder will be asked to attend to assist the Emergency Services in gaining access to the service user's home.
- Service users should be advised to only use door chains just before unlocking a door to answer a visitor, and to make sure they are removed before going to bed at night. Deadbolts should be discouraged – if the service user is worried about the physical strength of the door locks, additional key locks (such as 5 lever mortice locks) should be installed rather than using deadbolts.

Note: Service users should be reminded that an unlockable door chain or leaving a key in the door can delay access to a property.

- If the Emergency Services arrive before a nominated key holder/volunteer responder and there is no other means of access to the property (e.g. key safe with access code) then the Emergency Services may force entry.

6. ACCESS BY MEANS OF A KEY SAFE

6.1 Introduction

A key safe is a secure method of storing keys, and should be a robust device fitted to a property. The key safe has an access code to allow immediate access to the person's keys held within the key safe. The device is useful for people, who require multiple care visits, but have difficulty or are unable to answer the door due to physical disability or significant cognitive impairment.

A master key safe may be installed within sheltered, very sheltered and extra care developments; they are used to hold the master key for all flats. The key safe is linked via the warden call system directly to the Alarm Receiving Centre (ARC). Access to the key safe is provided via a numbered code. Where the key safe is linked via the warden call system directly to the Alarm Receiving Centre (ARC); the ARC can provide remote access.

The ARC will pass the access information to the response and/or Emergency Services when they are called to assist at the developments.

This section aims to provide information for the following areas:

- Guidance on a standard process for purchasing key safe
- Assessment
- Installation
- Code Management
- Using the key safe
- Decommissioning/Recycling

6.2 Purchasing a key safe

Consideration should be given to the following when commissioning the purchase of key safes (see Appendix 1):

- Security
- Installation
- Durability (weatherproof)
- Size – (dependant on the number of keys to be stored)
- Easy to use
- Can it be recycled?
- Ease of removal (from both a security perspective and the end-of-use perspective)
- Is there a Manufacturer's Guarantee
- Cost of the key safe
- Appearance/Look of the key safe (dependant on service user or landlord)
- After Sales Support
- Additional Features – Certification/Insurance (which may be required for insurance purposes)

6.3 Assessment

6.3.1 Outcome focussed assessment

A key safe should only be commissioned after alternative solutions that could assist the service user have been considered.

The outcome focussed assessment or review should consider whether the person being assessed:

- Is unable to reach the door safely due to severely restricted mobility or significant cognitive impairment.
- If the person lives alone.
- Is able to lock and unlock their door?
- Has had repeated no access to scheduled visits by care workers or other services
- Has difficulties that prevent them from opening their door to visitors and what risks are posed by the difficulties
- Could be supported by alternative solutions? (e.g. door entry system)
- Decisions should be made at the original assessment stage regarding who should take receipt of key from key safe when services end.

6.3.2 Eligibility

The purpose of the key safe should be to enable the service user's needs to be met by care services/providers and not be a device used for convenience.

Provision of a key safe may be considered for use by telecare response staff as the vast majority of alerts from people using telecare / telehealth are as a result of the need for assistance where they are not able to give access, for example if they have suffered a fall or are unwell.

6.3.3 Considerations

The safety aspects of having a key safe must be discussed and considered; for example, choosing a suitable location that avoids the key safe being visible to members of the public but being mindful that staff and others would be required to use the key safe. It would be good practice to choose a robust key safe model to minimise criminal activity such as removal of the key safe to obtain the key. Even when effective access code management procedures are in place, the possibility of a breach in information security could occur i.e. key safe access codes obtained by unauthorised people.

The following points must be explored, agreed and recorded in the assessment/review notes:

- How the key safe will be used
- Details of who the code can be shared with
- How the code will be kept safe by each person holding the key safe access code.
- Who will be responsible for handling key/s. (Installers would not be responsible for handling key/s unless detailed in their job description).
- Who will insert the key into the key safe.
- If the key safe is purchased by the person record how this will be managed and by who.

6.3.4 Permission /Consent – by the person to have a key safe

- The person should have capacity to give informed consent for the installation of a key safe and who has the access code. Assessors should ensure this is considered.
- If the service user is unable to provide consent or/ take informed decisions, permission to should be sought from a relative or person (next of kin) who has legal responsibility for the affairs of that service user before installation of the key safe
- Consideration should be given to the impact on the individual's home insurance before installation.
- Where the service user lives in rented or flatted accommodation, written permission to install a key safe must be sought from the appropriate landlord or other owner-occupiers.
- Organisations should have a signed service user agreement before installation takes place that includes details of who will be given the access code to facilitate access to their home.

6.3.5 Key safe information for service users and their family and carer

It will always be good practice to provide information to the individual and their family and carers. This information should be made available at the time of assessment/review.

6.3.6 Support Plan

It is recommended that any Support Plan should include the following detail:

- How the key safe will be used
- Who will have access to the key code e.g. care agency staff, Meals service, Social care or Patient transport, District Nurse or Emergency Services
- The continued need for a key safe should be addressed at each review. Where more appropriate, alternative solutions are identified and put in place, the key safe should be removed.

6.4 Installation

Service Providers should have procedures in place for the installation of key safes that meet the appropriate industry and market standards, with:-

- Staff undertaking the installation should clearly understand and follow the installation procedures as set out by the manufacturer's instructions, using the fittings supplied. Training, where required should be requested from the key safe supplier. *(NB this assumes that the key safe can be fitted to the property. If it cannot, then alternative options need to be explored.)*
- If the manufacturer's instructions cannot be complied with i.e. fitting onto structures that are wooden, have pebbledash or rendered walls, porous or crumbling brickwork, mortar, or buildings that are prefabricated, then installation of a key safe should be reconsidered.
- The key safe should be sited in a covert position that is easily accessible for all.

Service users should be given accessible information about the key safe that includes:

- installation
- access codes
- how the key safe will be used
- how their information will be stored

6.5 Key Safe Access Codes

Key safe access codes must be treated as highly confidential information. They should not be shared with anyone else unless authorised to do so by the service user e.g. relevant agencies and care staff providing support.

Organisations should have a policy for the safe use and storage of service users' information that meets data security legislation. Excluding the ARCs secure data base the key safe access codes must not be stored with the service user's name or address or with any identifiable information that would enable an unauthorised person to identify the address.

Staff responsible for installation and/or setting access codes should hold current membership of the Protection of Vulnerable Groups (PVG) scheme; subject to regular disclosure review.

The installer should not retain a record of the key safe access code, and should dispose of such information securely.

The service provider should have procedures in place covering:

- setting the access code number
- where access codes are stored
- who is authorised to view access codes
- who are agreed authorised access code holders (e.g. care staff)
- duties and responsibilities of authorised access code holders.
- measures in event of access codes being compromised.
- periodic change of access codes
- to manage codes in the event that a key safe access code holder member of staff leaves

The following best practice is advisable when managing codes for key safes:

- Manufactures guidelines are followed when stetting and using codes.
- The key safe access code can be entered in any sequence on a push button mechanical lock.
- Access codes should be unique to individual service users and their property. Dates of Birth / Telephone numbers, or any number that could be associated to a service user/Tenant should however be avoided. There should be no duplication of numbers or group numbers for a particular geographical area.
- Storing/carrying key safe access codes manually on written paper should be avoided
- Access codes should be restricted to authorised personnel as agreed with the service user, in order to reduce risk
- Access codes should be reset as a result of change in end user or suspected breach of security.

6.6 Responsibilities of a Key Safe Access Code Holder

Key safe access code holders are individual's with the designated authority to access a key from a key safe to enter a person's home, securing the property at the end of each visit.

It would be good practice to emphasise to the service user that **giving someone your access code is the equivalent of giving that person your house key**.

Organisations should have procedures in place that identify who is responsible for designating which staff will act as access code holders.

The access code holder must be fully aware of their responsibilities to ensure the security and safety of the service user and their home at all times in line with the National Care Standards.

All access code holders will be responsible for the confidentiality and security of the access code information at all times.

If the service user is not at home once access has been gained, the worker must leave immediately, secure the service user's property and return the key to the key safe. Additionally they should report that the service user was not home to their line manager and follow any associated procedures.

Should any access code become compromised (e.g. lost or stolen), the access code holder should inform their line manager and the service user and make arrangements to change the access code immediately. It may also be necessary for the police to be informed, particularly in the event of theft.

6.7 Removal of Key Safe

Organisations should have a signed service user agreement in place before removal takes place this should include details of who the key will be returned on termination of services. Families should be informed at the assessment stage that key safes might be removed when services are no longer required.

Staff responsible for removing and decoding the key safe should decode the key safe prior to returning to stock. (Staff must hold current membership of the Protection of Vulnerable Groups (PVG) scheme; subject to regular disclosure review).

The service provider should have procedures in place covering

- removing the access code number in any sequence (applies to a push button mechanical lock)
- where access codes are stored updated as “returned to stock”
- where and who the key was returned to
- measures in the event of access codes being compromised

The following best practice is advisable when removing key safes:

- If the service user did not live alone remove only after re-assessment, (possibility next of kin may require telecare/homecare/other services.
- Follow manufacturer guidelines on removal to ensure compliance with insurance/ accreditations
- Liaise/advise with families that the key safe will be removed in a timely manner at the end of services, if possible at the same time any other equipment is being removed.
- Removal should be requested in line with the service level/user agreement.
- Decontamination and cleaning should take place prior to return to stock.
- To ensure effective recycling / reuse of key safes the individual removing the key safe from the wall should reset the code to zero and not lock the unit using any codes as this renders the key safe unusable.

6.8 Recycling / Re-use

Most key safes can be reused after they have been removed, cleaned and deemed to be in a satisfactory working order. When reusing a key safe the staff undertaking the installation should clearly understand and follow the installation procedures as set out by the manufacturer’s instructions and ensure they use the manufacturer’s fittings. This means that a supply of spare fittings must be available.

It would be good practice to follow manufacturers’ installation guidelines provided with the key safe, as well as instruction received at training and the good practice guidance highlighted within the “Installation” section of this document.

In addition the following best practice is advisable when re-using a key safe:

- Prior to re-use of key safe carry out a maintenance check by testing code mechanics
- Technicians must ensure that fittings are renewed on key safes in line with manufacturers’ guidance to ensure compliance with any certification or insurance accreditation.
- When reusing key safes the same fittings cannot be used more than once.

7. MASTER KEY SAFE ACCESS

7.1 Introduction

Master key safes are used to facilitate access to developments/properties with multiple residents i.e. Sheltered Housing, the master key should only be used to gain access to the service user's home in an emergency.

7.2 Location

Consideration should be given to the location of the master key safe/cabinet in direct relation to off-site warden call systems communication/speech modules to minimise call interference.

7.3 Restricted Access

Access to key safe/cabinets containing the development master key is restricted to on site staff within the developments, Emergency Services (Fire, Police, and Ambulance), GP, District Nurse, Housing Association staff, Responder services or emergency contractors if they have been called out by the ARC **providing agreed service or agreement otherwise made**. An attempt should be made to contact the person being visited to forewarn of an emergency contractor visit if access to the master key is given.

7.4 Returning key

Each time access granted to the master key safe/cabinet the visiting service must ensure the key is returned to the key safe. There should be an agreed protocol for ensuring the key is safely returned to the key safe/cabinet and that on site staff are advised when access has been granted to give the opportunity for access code changes if deemed necessary. Any non-return of a master key or suspected security breach should be highlighted to on-site staff and the organisation concerned.

7.5 Special considerations

It would be good practice to alert the nominated contact and development staff or organisation if access is granted when the person is out or away from their home.

8. ACCESS USING KEYS HELD BY AN ORGANISATION

8.1 Personal Information

Access to the service user's personal information, including address and any security measures, such as intruder alarm codes are to be kept in a secure and confidential manner in line with the organisational security protocols. It would be good practice to have password protected computer systems, encrypted files or locked cabinets with restricted access by authorised staff. Sharing of the information/ allowing other services access to the service user's keys can be done only by prior consent.

8.2 Key Management

It would be good practice to consider the following when storing and handling keys belonging to service users:

- When keys are received from the service user a receipt should be issued detailing those keys entrusted to the Telecare service provider. One copy of the receipt should be given to the service user and one copy should be retained by the Telecare service provider. (Some Telecare Services scan a copy into the service user record held on the ARC system).
- The receipt should include:
  - o Name, address and telephone number of the service provider
  - o Date and time of key exchange
  - o Description of keys, including number of copies
  - o Name of owner
  - o Name of person receiving the key/s
  - o Signature of both service user and staff member
- Keys must be kept in a lockable safe, with access restricted to authorised staff only.
- No names or addresses are on the keys, they are given their own ID code number which correlates with the person's ID on their secure manual file or on the password protected computer system.
- Access to keys is limited to the Telecare staff only, for requests for keys by other staff, it would be good practice to have a process in place (via the Telecare team manager) to ensure a full explanation on why the key request has been made and provided. Permission to share the keys with other professionals will be with the service user's prior permission.

- Staff handle the keys in a safe manner at all times, when out on a Response Visit/follow up visit, staff must store keys as discreetly as possible.
- Keys carried in a vehicle should not be left in plain view when travelling and should not be within reach of an unlocked door or open window.
- Keys should be kept with the Responder at all times when leaving the vehicle or stored securely within the vehicle. The vehicle should always be locked when left unattended.
- If vehicles are used to store keys at any time, then the physical size and strength of the vehicle construction should determine the limit to the number of keys stored or carried.
- It would be good practice to have secure storage within the vehicle e.g. a key safe which is not visible externally, which can only be accessed from inside the vehicle, is separately locked with no removable or glazed panels.
- When the keys have been returned, they must be stored in the same place in the safe to ensure they can be found and re-used.
- Each issue or use is recorded on the Telecare Service records for each service user this includes which member of staff has used the keys, why they used the key/s and the date.
- Any changes in responsibility for the keys are recorded on the service user record.
- Daily checks are made and signed confirmation by staff to state keys have been checked and accounted for.
- Archived service user records have a note of the key receipt.
- Efforts are made to return the keys to the owner or, next of kin if this fails the unclaimed keys are removed from the safe and held in a separate box, these are disposed of in line with local policies and procedures or by logging onto www.recyclenow.com
- It would be good practice when disposing of keys if unable to return them, to ensure the method chosen renders the key unusable, unrecognisable and impossible to copy or duplicate.
- In the event of keys being lost or stolen, staff should inform their manager at earliest opportunity, the manager should contact the relevant service user to inform of this and re-assure that no identifying names or addresses are on keys.
- The Telecare Service would discuss changing the lock/s and would meet all costs associated with this. The manager organises lock change and arrange to collect new key/s
- Returning keys, this is done by a Telecare Service staff member who contact's service user and/or their family/next of kin/carer in advance and arranges for the keys to be returned, the key receipt is signed and dated by both service user or their representative, telecare staff and recorded on the service user's file.
- Staff who do not follow the procedure for the safe storage, handling and return of service users keys maybe subject to disciplinary proceedings.

9. REMOTE ACCESS

9.1 Introduction

ARCs may receive calls from people or on behalf of someone who requires help and is in a location where access has to be facilitated e.g. a woman with dementia is found by the police in the street, she is able to tell them her name, address and date of birth. The police take her back home to the sheltered housing complex; they press the warden call system linked through to the ARC. The ARC verifies the police officers are genuine by calling the police force control centre (dial 101). When the ARC has confirmed the authenticity of the police officers they provide access to the complex and to the master key safe to allow access to the woman's home.

9.2 Guidance on access

ARCs have monitoring equipment that identifies the type and location of calls, or in the case of a call on behalf of another person may hold a record relating to that person. Calls are answered by trained calls handlers who will take appropriate action, which may include calling various categories of responders including the Emergency Services and giving guidance on how they should gain access.

Guidance should be held securely, checked regularly particularly following any incidents where access is difficult, and forms an important element of risk assessments of individual Telecare installations or risk assessments of buildings (e.g. risk assessments of sheltered complexes).

The quality of the guidance held is important. It must be clear and succinct and there should be call handling procedures for passing information regarding access at the point of calling any responders including the Emergency Services.

9.3 Access by Emergency Services and other personnel

Service users should have a clear understanding of when and to whom access will be given to anyone and that decisions taken may override their wishes, for example when the Fire and Rescue Service are called in response to unexplained calls triggered by fire detection equipment.

ARCs will facilitate access to the Emergency Services in ways that they will not for other persons, for example giving either remote access to (or codes to open) doors or key safes containing master keys that open the doors of residents' flats in housing complexes. Concerns for the vulnerability of service users and security of property underlie this important distinction in how access might be given differently to various people. Typically a maintenance contractor may be given access to a digital key safe containing keys for maintenance purposes.

9.4 Testing and maintenance of digital key safes

When access relies on equipment this equipment is regularly tested and records of testing held. Testing is undertaken when equipment is installed, replaced or upgraded including when an alarm receiving centres equipment is modified in a way which may affect their ability to remotely control equipment.

Maintenance agreements should be in place to ensure that faults with equipment that is essential for facilitating remote access are treated as emergency repairs.

9.5 ARCs risk management

ARCs must be resilient and have business continuity arrangements that ensure emergency access can be given at any time. This includes local business continuity plans for when local equipment faults prevent calls being received by monitoring centres.

9.6 Methods of access

9.6.1 Digital Key Safes

It is important that there is more than one method of ARCs facilitating access. The method of giving access to the Emergency Services may be different due to the building and equipment in place, i.e. the core and cluster housing model *(The core-cluster housing model consists of a network or "cluster" of residences which are linked to a "hub" or "core" residence)* which may have and external key box, but whatever the method there has to be a recovery process for when that method fails. Should remote access not be possible or a digital access code not work due to technical failure, guidance must be given on how access may then be achieved.

Some ARCs give the Emergency Services access codes for main door entries when calling them to attend housing complexes with grouped warden call systems. This is to prevent any delay in them gaining immediate access. This also means it does not matter if the equipment is "on site" or "offsite" at the time the Emergency Services arrive.

When access is given to master keys there must be a procedure in place to ensure those keys are returned to the key safe.

Remote access via door entries to other persons must be highly controlled by application of calls handling procedures. Access is given only when authorisation is recorded. ARC should have regard for the privacy of service users and do not operate a concierge service with the exception of when a caller is a carer or other person with whom they had a pre-arranged appointment.

9.6.2 Main Door Access

Accessible entrances are usually fitted with enquiry panels that mostly give visitors or visiting services the option to call into the person's home. The panels will have an overall enquiry function or manager button that will link to on site staff if available and to the ARC at all other times.

If the enquiry panel is activated off site to the ARC it would be good practice to consider this practice;

- Request name of visitor & purpose of visit
- If no speech, make a second attempt to request details, if no response, close call
- 999/GP access required, usually the ARC will have requested the attendance of the Emergency Services and will be expecting the door activation and will allow access
- 999 / GP access where the ARC has not requested the attendance of the Emergency Services should check the authenticity with person being visited or the centre controlling the requestor services (999 call back /NHS24 / GP Surgery)
- Visiting services / career / visitor requesting access it is good practice to have an agreed process for access notes or on-screen instructions to allow or deny access.
- The ARC upon receipt of a door call should check access notes or on screen instructions are followed/ checked for requirements or password notes, checking with the person being visited is also an option
- CCTV can also be linked to the ARC to check authenticity of calling services. This additional means can aid the security of people's homes especially in the case where specific visitors are to be denied access by the ARC.

- Caution must be taken before giving access. If no notes/authenticity are available then, no access should be given before identity is checked

Alert: If the ARC call handler suspects that the person being visited is unsure of the identity of their visitor and their request for access then the ARC should call the key holder or nominated contacts for verification.

9.6.3 Door Entry / Access Control Systems

Door entry / access control systems, such as those which use fobs or cards are in many respects similar operationally to access using keys i.e. they may be thought of as electronic key systems.

They are important in facilitating easy access particularly for people who may otherwise experience difficulty and include door openers which may be triggers that operate via grouped or dispersed social alarm equipment.

The benefit of some access control systems is that they allow for different levels of access (i.e. the level of authorisation can be programmed in differently for different persons) access can be removed should there be a security concern similar to a lost key and there is no need to change locks (or an entire suite of locks!). The principle of least privilege is applied with access control systems i.e. each person only has the access they require.

An important benefit is that access does not rely on an ARC giving access. This is particularly beneficial for carers who may otherwise spend time waiting for door entry calls to an ARC being answered.

As technology advances methods of controlling access become easier and simultaneously the need for control increases. For example some grouped warden call equipment can be programmed via web interfaces which allow for access codes to be remotely changed. This is important in responding to security concerns and also reducing the need for anyone to attend to site to perform the same task.

Social alarm, telecare equipment and ARC equipment that allows for video communication has application in terms of checking credentials of anyone seeking access, and reduces the risk of tailgating (a term used in the security industry for someone entering immediately after another person).

Access control systems are equipment that should be maintained on the basis of any repairs being treated as priority repairs.

9.6.4 Barrier Free Access

Barrier free access is where the highest standards of access and inclusion are developed through new building and re-development of existing housing throughout Scotland. New developments or adaptations to existing developments must be responsive to people's needs, offer choice and fully understand the challenges and barriers to access. Many of the measures taken singly increase access and when combined can provide an environment where people can continue to lead independent lives and be supported as their individual circumstances change. Homes within design control or adaptations policies should consider people's needs in relation to their access requirements. Such as:

- General environmental adjustments for the benefit of all building users;
- Personal needs-assessed alterations and adaptations;
- Clear internal and external signage with clearly defined entrances to help make buildings visible;
- Lowered kerbs to enable street access;
- Accessible entrances with power operated main doors.
- Enquiry panels at the main entrance to provide a direct link to individual flats via the warden call system. This ensures communication with the service user, check all is well, notify of transport, and respond to an emergency.
- If unable to contact the person the panel can link to the development staff or to an ARC. Visiting services are registered with the ARC to expedite entry to the development and 999 services are advised upon requests for attendance that the development main entrance door and key cabinet / master key will be remotely released by the ARC.
- A development key safe should be installed that holds the master key for all flats. The key safe should be linked via the warden call system directly to the ARC when no staff available on site to enable remote opening for emergency access.

Personal key safes are fitted when required outside the entrance to individual flats to allow access to a wide range of attending outside services the ARC may or may not hold the access code to individual key safes.

10 ACCESS BY FORCED ENTRY

10.1 Introduction

There are occasions where forced entry is the only option. Usually because there is no key safe, there are no local key holders or keys are unavailable to enter the property. Forced entry should be a last resort and should only be used when all other access options have been explored or there is a significant risk to life if access is delayed.

Where access is required Police Scotland should be called.

10.2 Police Scotland Standard Operating Procedure on Forced Entry

Under Section 20 of the Police and Fire Reform Act (Scotland) 2012 Police Officers may force entry to a premise to Protect Life and Limb.

Police Officers can also force entry under common law to Protect Life and Property.

On arrival Police Scotland will liaise with those present and carry out all appropriate enquiries to confirm the necessity for forced entry and the options available to gain access without it, unless immediate access is required.

The officer present must consult with their supervisor to confirm forced entry before continuing.

If there is no immediate need for Police Scotland to force entry, the officer should make all necessary enquiries with the relevant persons and agencies present to establish there is a need to force entry. If there still appears no immediate need to gain access or risk to life by delaying access then Police Scotland would recommend that a joiner is called out.

Where Police Scotland force entry using statutory or common law powers the responsibility for any costs falls to the owner / occupier of the property or they may be recoverable from the person's insurance company.

There may be occasions where there is another statutory agency with similar powers present, for example Fire and Rescue Service etc. Where they are the lead agency Police Scotland will support them to gain entry.

APPENDIX 1: ACCESS TO SERVICE USERS HOMES – KEYSAFE

COMMISSIONING

CONSIDERATION	
WHAT TO LOOK FOR	Police Sppproved Secure By Design; Durability (Weatherproof); Size for Volume of Keysafe; Can it be recycled; Manufacturers Guarantee; Cost of Keysafe; Appearance and look of keysafe
ACCESSORIES	Code Cover, replacement SBD screws
CONSIDERATIONS TOWARDS THE USER OF THE KEYSAFE	Dexterity; Visual Impairment; Mobility
AFTER SALES SUPPORT	Dedicated Supplier support team and face to face meetings
TRACABILITY OF KEYSAFE	Asset Management; CRM Systems; Serial Numbers
CONVENIENCE v's SECURITY	LPS1175 Accreditation; Testing; SBD Accreditation
ADDITIONAL FEATURES	Is it recognised by Insurers?

CODE MANAGEMENT

CONSIDERATION	
CODING THE KEY SAFE	Avoid date of births; always use 5 digit code including A or B
WHO HAS ACCESS TO THE KEY SAFE?	Community Alarm Emergency Responders; Homecare Services; Long Term
STORING A CODE	Secure database; CRM System
WHO IS INVOLVED IN SET UP?	Social Work; Community Alarms

DECOMMISSIONING/RECYCLING

CONSIDERATION	
WHEN IS DECOMMISSIONING SUITABLE?	See Re-Assessment; possibility next of kin may now require homecare/services
COMMUNICATION AND TIMING	Manufacturer Guidelines to be followed; Guidance from supplier and De-install/ Re-install protocol ie New SBD fixing screws must be used. Discuss with family and individual. Advise when service is no longer in use for removal of Key Safe
WHO IS COMMISSIONING?	Social Work; Housing; Handy Person Service; Private
DECONTAMINATION/ CLEANING	Medical Wipes; WD40
REMOVAL OF KEYS	Return key to family
REMOVAL OF CODES	Set to uncoded before returning of stock

ASSESSMENT AND INSTALLATION

CONSIDERATION	
COMMUNICATION	Manufacturer guidelines to be followed; Guidance from Supplier and De-install/ Re-install protocol ie New SBD fixing screws must be used. Discuss with family and individual and provide an information leaflet
WHO WILL CARRY OUT ASSESSMENT FOR KEYSAFE?	Assessment Team; Telecare/Telehealth; Mobility; Social Work xxxxx Any others to be added
HOW THE KEYSAFE WILL BE USED	Homecare Services; Emergency Responders; Services; Community Alarm
WHO INSTALLS THE KEYSAFE?	In-house department/handyperson service/ care and repair. NOT RESPONSIBLE FOR HANDLING KEYS UNLESS STATED IN JOB DESCRIPTION. PVG Checked; Experienced; Following guidelines and training given by Key Safe Supplier
HEALTH AND SAFETY	Location; Height
SUBSTRATE/FIXINGS	Follow installation guidelines and training given by Supplier Support Team
ASSET MANAGEMENT	Record install details, batch numbers and stock levels. Agree review and audit date
PERMISSION FROM LANDLORD	Written permission from the landlord or shared owners should be sought prior to installation
PRIVATE PURCHASE OF KEYSAFE	How will this be managed and by who?

USING THE KEY SAFE

CONSIDERATION	
PERIODIC AUDIT/ RE-EVALUATION	Agree timescale: Monthly/Quarterly/Yearly of if possible at the same time as Telecare Equipment Audit. Is Keysafe system still suitable and fit for purpose? Does the key still open lock? Is the keysafe code still the same? Update on who has the code? Is location still suitable?
CARE AT HOME	TO BE ADDED
REPLACE AFTER USE	SEE GPG SECTION

REFERENCES

http://www.gov.scot/resource/0041/00411586.pdf – A National Telehealth and Telecare Delivery Plan for Scotland to 2015

http://www.gov.scot/Resource/Doc/349603/0116844.pdf ;– National Care Standards at Home - Scotland

http://www.legislation.gov.uk/ukpga/1998/29/contents – Data Protection Act 1998

TSA GOOD PRACTICE GUIDE

Telecare Services Association Membership Services Centre Suite 8 Wilmslow House Grove Way Wilmslow Cheshire SK9 5AG
Telephone 01625 520320 www.telecare.org.uk