

CODE OF PRACTICE

FOR

THE PUBLIC EMERGENCY CALL SERVICE
(PECS)

**BETWEEN COMMUNICATIONS PROVIDERS, CALL HANDLING AGENCIES
AND THE EMERGENCY AUTHORITIES**

June 2020
Version 2.3

GLOSSARY OF TERMS	4
DOCUMENT OWNERSHIP AND REVIEW	5
1. GENERAL INFORMATION	6
2. QUALITY OF SERVICE (GENERAL)	7
3. PROCESS FOR CALLER CONNECTION TO THE CORRECT EA	8
3.1 THE CALLING CUSTOMER	8
3.2 EA SELECTION	8
3.3 DELIVERY OF THE CALL TO EA CONTROL ROOMS	9
4. DIFFICULTIES CONNECTING TO THE EACR	10
4.1 CRITICAL CONTACT NUMBER	10
4.2 BUDDY EA	10
5. CONTINGENCIES AND REVIEW OF EACR NUMBERS	11
6. CALL QUEUING SYSTEMS AT EACRS	12
6.1 QUEUE SET UP	12
6.2 QUEUE ANNOUNCEMENT/MESSAGE	12
7. CALL MONITORING AND DISCONNECTION	13
7.1 EA REQUIRES FURTHER INFORMATION	13
8. CALLS WITHOUT SERVICE REQUEST	15
8.1 CALLS WITHOUT SERVICE REQUEST FROM MOBILE PHONES	15
8.2 112 CALLS WITHOUT SERVICE REQUEST FROM FIXED PHONES	15
9. POST-CALL PROVISION OF CALL AND CALLER INFORMATION	17
9.1 PROCESS	17
9.2 THE EMERGENCY PERIOD	17
9.3 CONFIDENTIAL CUSTOMER INFORMATION	18
9.4 MOBILE PHONE SUBSCRIBER CHECKS	18
9.5 MOBILE VIRTUAL NETWORK OPERATOR (MVNO)	18
10. MISROUTED CALLS AND MOBILE ZONE PROBLEMS	19
10.1 BOUNDARY OVERLAP (Mobile ECNs)	20
10.2 FAILURE TO DISPLAY ZONE OR CELL ID INFORMATION (Mobile ECNs)	20
11. ROUTING METHODS AND FAULT MANAGEMENT	21
11.1 ROUTING METHODS AND NETWORK SECURITY	21
11.2 PRIORITY FAULT REPAIR SERVICE	21
11.3 ISOLATION OF CUSTOMERS DUE TO NETWORK FAILURE	21
11.4 DRAFT MEDIA STATEMENT FOR CHAs/CPs AND EAs	22
12. MANAGEMENT OF MAJOR INFLUXES OF EMERGENCY CALLS	24
12.1 ADVANCE WARNING OF MAJOR INCIDENTS	24
12.2 CONTACTS	24
12.3 MODIFICATIONS TO QUEUING SYSTEMS	24
12.4 CHANGES TO CALL HANDLING PROCEDURES	25
12.5 MEDIA ANNOUNCEMENTS DURING A MAJOR INCIDENT	26
13. RECORDING OF CALLS	27
14. OTHER TYPES OF CALLS	28
14.1 LIMITED SERVICE STATE EMERGENCY CALLS	28
14.2 TEXT RELAY (Previously Text Direct/Typetalk)	29

14.3 eSMS	30
14.4 eCall AND TELEMATICS EMERGENCY CALLS	31
14.5 OTHER VEHICLE ACTIVATIONS	32
15. NUISANCE AND HOAX CALLS	33
APPENDIX 1: CHA CONTACT DETAILS	35
APPENDIX 2: CELLULAR RADIO COMPANIES CONTACT DETAILS	36
APPENDIX 3: GUIDANCE ON USE OF LOCATION INFORMATION	37
APPENDIX 4: BEST PRACTICE GUIDE FOR CPs ON NAME & ADDRESS INFORMATION	41
APPENDIX 5: MANAGEMENT OF MAJOR INFLUXES OF CALLS - CONFERENCE CALL INVITE AND AGENDA	43
APPENDIX 6: MOBILE DISCONNECTION	44
APPENDIX 7: IPA REQUEST FOR DATA	45
APPENDIX 8: EMERGENCY CALL MISROUTE AND DETAILS DISCREPANCY	46
APPENDIX 9: HOAX VOIP CALLS WITH NO ADDRESS DETAILS	48
APPENDIX 10 EMERGENCY ROAMER ADDITIONAL PROCESS INFORMATION	49
APPENDIX 11 :ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA CODE OF PRACTICE (PURSUANT TO IPA)	50
ANNEX 12: eSMS MEMORANDUM OF UNDERSTANDING	52
ANNEX 13: TELEMATICS PROTOCOL	53

GLOSSARY OF TERMS

999/112 Liaison Committee	Committee facilitated by the Department for Digital, Culture, Media and Sport which brings together Emergency Authorities, Government Departments, Call Handling Agents and Communications Providers to consider matters of common interest.
AML	Advanced Mobile Location
BAPCO	British APCO
BT	British Telecommunications plc
Caller Location	Any data or information processed in an Electronic Communications Network (ECN) which gives the geographic position of the terminal equipment of the person making the emergency call.
CAD	Computer Aided Despatch
CCN	Critical Contact Number
CHA	Call Handling Agent
CLI	Calling Line Identity
COCOM	Committee on Communications
CP	Communications Provider (or TO) is an organisation that provides an ECN or an ECS . This term is used within the Communications Act 2003.
DDI	Direct Dial In
DEIT	Direct Electronic Information Transfer
EA	Emergency Authority
EACR	Emergency Authority Control Room
ECN	Electronic Communications Network
ECS	Electronic Communications Service
EISEC	Enhanced Information Service for Emergency Calls
Emergency Caller	A 999/112 caller
Emergency Roamer	A 999/112 caller using a network that is not their home network – also called Limited Service State (LSS)
EO	Emergency Operator
eSMS	Emergency Short Message Service
IMSI	International Mobile Subscriber Identity
IPA	Investigatory Powers Act 2016
LSS	Limited Service State
MAIT	Multi Agency Information Transfer
MET AUTO	Voice response system hosted by the Metropolitan Police Service
MNO	Mobile network operator
MSC	Mobile Switching Centre
MVNO	Mobile Virtual Network Operator
NPCC	National Police Chiefs' Council (formerly ACPO)
OC	Operator Centre [Fixed Network]
PECS	Public Emergency Call Service
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
TO	Telecommunications Operator – synonymous with CP . This term is used within the Investigatory Powers Act 2016.
URN	Unique Reference Number
VoIP	Voice over Internet Protocol

XD
TECSOS

Ex-directory
A call type for vulnerable callers

DOCUMENT OWNERSHIP AND REVIEW

This document is owned by DCMS on behalf of the 999/112 Liaison Committee.

It will be reviewed at least annually from December 2019.

1. GENERAL INFORMATION

This Code of Practice (“the Code”) is intended to deal with the method of handling '999/112' public emergency telephone calls between the Call Handling Agents (“CHAs”) and the Emergency Authorities (“EAs”) in the UK (Police, Fire, Ambulance and Coastguard).

The Call Handling Agents (see Appendix 1) and the Emergency Authorities have agreed the contents of the Code through the auspices of the 999 Liaison Committee. The Code is subject to regular review by the 999 Liaison Committee who will arrange for copies to be distributed to the CHAs and to all EA Chief Officers.

All Communications Providers (“CPs”) have obligations under the Communications Act 2003, implemented under Condition A3 of Ofcom’s General Conditions of Entitlement in respect of emergency calls made to 999 and 112.

The CP must ensure that any end user can access EAs by using the emergency numbers “112” and “999” at no charge and, in the case of a pay telephone, without having to use coins or cards. In the case of mobile networks, enabling 999 or 112 emergency calls to be made from mobile telephones which do not have radio coverage from their normal Network Provider is expected to allow the public to maximise chances of quickly making an emergency call. These calls are variously known as ‘displaced’ calls, “emergency roamers”, “camped” calls, or Limited Service State calls. These calls will be referred to as Emergency Roamers throughout this document but it should be noted that the CHA operators will refer to them as Limited Service State calls at hand over to the EA control rooms to quickly convey that call is not on its home network.

The CP must also make caller location information available to the EAs, to the extent technically feasible, for all calls to the emergency numbers 112 and 999. ‘Caller Location’ is defined as any data or information processed in an Electronic Communications Network (“ECN”) which gives the geographic position of the terminal equipment of the person making the emergency call. Note in the case of Emergency Roamer calls no valid Calling Line Identity (CLI) will be passed from the ECN.

The CPs deal with the requirement to provide a Public Emergency Call Service by contracting with a Call Handling Agent (CHA). In the UK BT currently acts as CHA for all the networks.

The handling of an emergency call by a CHA involves the five main phases:

- Connection of the caller over the CP and CHA networks to the CHA’s Emergency Operator (“EO”) via the 999/112 number.
- Selection by the emergency operator of the required EA Control Room (EACR).
- Onward connection of the caller to the EACR over the CP/CHA networks.
- Listening by the EO to ensure that connection has been established with the appropriate EACR and the ability to provide further assistance to the caller or Emergency Authority (EA) when required.
- Provision of location information

2. QUALITY OF SERVICE (GENERAL)

Under present legislation there are no quality of service standards laid down for 999/112 call handling by CHAs or the EAs.

The CHAs have a target of answering 95% of 999/112 calls within 5 seconds. To meet this commitment, 999/112 calls receive priority by CHA EOs over all other calls. If the EO has any other call in hand when a 999/112 call arrives the operator will ask that caller to hold the line and will deal with the emergency call.

In the same manner, the EAs place the highest priority on incoming emergency code calls. All such calls are treated equally with no discrimination between fixed line and mobile callers.

EAs are subject to recommended attendance/response times. The Police Service aims to answer 999/112 calls within 10 seconds; the recommended response time for the Ambulance Service is to answer 95% within 5 seconds, Scottish Ambulance 90% in 10 seconds; the Fire and Rescue Service and the Coastguard aim to answer 95% within 10 seconds.

CHAs and EAs performance will be presented (through figures gathered centrally) at each 999/112 Liaison Committee meeting. Fire and rescue services for England are not routinely presented. Should statistics be required for a particular issue or FRS then best endeavours will be made to present them.

3. PROCESS FOR CALLER CONNECTION TO THE CORRECT EA

3.1 THE CALLING CUSTOMER

Before connecting a call to the relevant EA, CHA EOs will obtain, or seek to obtain, from the 999/112 caller

- (i) which EA the caller requires (i.e. fire, police, ambulance, coastguard).
- (ii) the telephone number of the caller. If the caller's telephone number is not automatically available and the caller cannot provide it, the EO will ask for the approximate location of the caller and seek to connect the call to the appropriate EA. Under no circumstances will the CHA EO refuse to onward connect an emergency 999/112 call.

It is the responsibility of the EACR staff to obtain adequate address information from the caller to enable the EACR to locate the incident being reported.

Multi-Agency Calls

If a customer makes a request for more than one EA the CHA operator will connect the customer to the first EA requested and provide a verbal handover stating that the customer has requested more than one service (and advise which one).

The EA controller will confirm to the CHA operator during call handling that they will pass details to the other EA(s) and do so using existing processes. If the EA controller is unable to do this on occasions, they will request the CHA operator to remain on the call and onward connect to the other requested EA(s). They may ask the caller to stay online at the end of the call so that, when the EA clears, the call will be represented to the CHA 999 operator for further connection to the other service(s). When the first EA ends their call, and the caller stays online, the call will be represented back to the CHA, who will then ask which service is needed and connect to the next EA required. However, this service will only work if the call was connected to the EA over a non-analogue connection.

3.2 EA SELECTION

When a CHA EO answers an emergency call, the full national calling number (except in the case of emergency roamers – see **Section 14.1**) and for mobile calls the zone code (group of cells) or Cell ID, will normally be automatically displayed on the operator's console. For 999/112 calls this calling number will be displayed on the operator's console even if the caller withheld their number.

The EACR routings automatically displayed are based on matching the EACR areas to the calling number's postal code (or in absence of a postal code the exchange catchment area or nearest town information) for fixed calls, and to the zone code or Cell ID for mobile calls. The list of EACR routings shown is agreed between the CPs, the CHAs and the EAs. This information is updated as necessary to account for number changes, new cells etc.

There are a small number of cases where callers will need to be asked for their number, or asked to confirm their location, in order to display the correct EACR routing. These cases include (a) Alarm Monitoring Centres forwarding calls from their clients, (b) when a Voice over Internet Protocol (VoIP) terminal is being used, (c) when a default number has displayed due to an exchange working in fall-back mode (d) where a PBX extension user is displaying the main number

3.3 DELIVERY OF THE CALL TO EA CONTROL ROOMS

It is the responsibility of the EAs to provide the means of receiving emergency calls and keep the 999/112 liaison contact point in the CHA informed (see Appendix 1) of the equipment and connect-to routings in use in the EACRs.

To cater for unforeseen circumstances EAs will provide three separate routes.

Primary

This is the route that the CHA operator will initially use to connect a caller to the EACR and the EA must provide sufficient capacity on this route to handle normal 999/112 traffic distribution. EAs will reserve primary routes exclusively for receiving 999/112 calls.

Secondary

In circumstances where the CHA emergency operator receives no reply on the primary number after 60 seconds (or 2 minutes where a queue is in use) the operator will connect the call to a secondary number provided by the EA. This procedure should only be necessary in instances when the EACR has an unusually high level of traffic, or a fault in its system or in one of the ECNs.

Alternative

In the event of a major problem which results in the primary and secondary routes to an EACR being unavailable to the CHAs, including a further period of 30 seconds of no reply on the secondary number, the EA should provide the CHAs with an alternative means of taking delivery of the call,

To provide adequate resilience this alternative number must be served by a different network route from that providing the primary and secondary routes, ideally at a different EACR for maximum resilience. EAs must consider, where appropriate, which EACRs are used as alternatives to each other.

Notes:

- Mobile CPs and the Cabinet Office do not advise the use of a mobile phone as an alternative route.
- The EA and its CP(s) need to liaise regularly to ensure that there is no single point of failure affecting both the primary and secondary routes.
- The same primary, secondary and alternative numbers should be used for all 999/112 calls, whether fixed or mobile, and regardless of which CHA connects the call.
- All the routes will need to be staffed on a 24-hour basis.

4. DIFFICULTIES CONNECTING TO THE EACR

4.1 CRITICAL CONTACT NUMBER

EAs need to provide the CHAs 999/112 liaison contact point (see Appendix 1) with a 24hr critical contact number (CCN) within the EACR to be used only when Operator Centres are having difficulty connecting calls to the EACR. This number will only be used for CHA Operator Centre managers to contact EACR managers in the event of 999/112 call handling problems relating to call surges, call answering times, staffing difficulties, or other problems so that corrective action can be agreed. For example, Operator Centre managers will call if there are extended delays in an EACR answering of about 5 minutes or where there are delays and they have an exceptionally critical call waiting.

Notes:

- To ensure EACR managers receive the minimum number of calls, it will normally only be one BT centre that calls, and they should then cascade relevant information to other centres.
- If the CHA Manager is unable to contact the EACR Manager on their Critical Contact number, then they will speak to: -
- a neighbouring EACR of the same type (preferably a “buddy EA” – see below) as first choice to see if they can help by either offering callers advice on line, or passing prioritised details back to the original EA (perhaps using radio), or maybe even responding in border areas;

or

an EACR that covers the same area (but of a different type) as second choice as they may be able to pass prioritised details back to the original EA (perhaps using radio), or will at least be able to offer more help than the CHA to very distressed callers

4.2 BUDDY EA

EAs need to pre-nominate an appropriate “Buddy EA” for the CHAs to use. “Buddy EAs” are expected to be used to assist in times of unexpected pressure and improve the speed of implementation and the effectiveness of contingency arrangements at such times by, for example, selecting “buddies” which allow call data to be readily transferred back to the original EACR.

Please note this links with Section 12 Management of Major Influxes of emergency calls

5. CONTINGENCIES AND REVIEW OF EACR NUMBERS

EAs should prepare contingency arrangements to cover the receipt of emergency calls during conditions of serious breakdown either in the ECN or the EA communications system. These arrangements must be planned to cover every control centre which normally receives emergency calls and should be tested periodically to ensure that both CHAs and EA staff are familiar with them. The EAs should make use of automatic call diversion facilities where possible.

CHAs and the EAs should regularly monitor the efficiency of the 999/112 emergency call arrangements and arrange regular liaison meetings at both national and local levels.

The EAs should inform the 999/112 liaison contacts points in all CHA's (see Appendix 1) of all changes to any EACR connect-to numbers giving a minimum of two weeks' notice. In the case of EA geographical boundary changes, at least one months' notice should be given along with full written details of the changes. The date and time of all such changes should also be given.

The CHAs 999/112 liaison contact points should also give the EAs a minimum of two weeks' notice if their own contact numbers change. This information should be notified direct to the EAs.

6. CALL QUEUING SYSTEMS AT EACRs

6.1 QUEUE SET UP

If the CHA operator is connected to a call queuing system, by clearing the original connection they are only placing themselves further back in the queue of calls and worsening their chances of being answered. To avoid this eventuality, the EA must notify the 999/112 liaison contact point in all the CHAs (see Appendix 1) when planning to introduce or change a call queuing system. This is so the CHAs can amend their information to advise operators a queue is in use.

If a number is known to enter a queue CHA operators will be instructed to try it for 2 minutes before setting-up to the secondary and/or alternative number. The CHAs need to know which of primary, secondary and alternative numbers are in a queue, whether the separate numbers enter the same queue, and whether the separate numbers all have the same priority within the queue.

If the primary and secondary numbers are in a common queue, the secondary should be given priority in that queue, thereby recognising that a call attempt has already been queued for 2 minutes and keeps its queue position while trying a different line.

6.2 QUEUE ANNOUNCEMENT/MESSAGE

The provision of a short acknowledgement message, or distinctive answer signal/tone, must be used by the EAs to inform both operators and callers that their calls are being held in a queue.

The queuing announcement/acknowledgement message should normally only be heard after at least 10 seconds of ringing tone, so that most callers would not hear it.

The announcement needs to terminate as soon as an EACR call taker becomes available and is presented with the call.

The recommended text for an announcement is as follows: - "You are connected to the Police/Fire/Ambulance Coastguard Service for emergency calls. We are currently receiving a high volume of calls. Please hold the line to report your emergency and you will be connected as soon as possible." Where this is not appropriate, e.g., when reporting a fire, any announcement will have to be thought out very carefully.

Following an announcement, ringing tone should again be provided and the announcement repeated at regular intervals until the call is answered.

If it is not possible to use an announcement, then use of a distinctive tone to indicate that the call has been placed in a queue at the EACR needs to be used. This could either be a variation to the normal public network ringing tone, or a periodic interruption of normal ringing tone (being provided by the EACR switch) by a different burst of a distinct tone.

Note: If possible, and the queuing system allows, extra information can be temporarily inserted into an announcement to try to manage demand and caller expectations. For example:
".....We are currently receiving a high volume of calls due to (major incident details)"

7. CALL MONITORING AND DISCONNECTION

Once the EA answers, the CHA EO will (unless interrupted by the caller) give the name of their Operator Centre (to facilitate recall), the caller's number and advise if it is a payphone or mobile caller. They will also advise the EA if:

- the caller's number is not known.
- the caller is an emergency roamer
- the caller is a TECSOS user (vulnerable caller)
- it is a Telematics call

CPs are required to provide location information to the emergency services for 999/112 calls and this is made available to EAs via the BT CHA's location "hub", known as the EISEC hub (Enhanced Information Service for Emergency Calls). To allow EAs to access locations, the caller's number and the Operator Centre identity** are automatically transferred to the EACR's switch and do not need to be verbally passed, however, verbal handover will still be given in the circumstances listed in the bullets above.

EAs are then expected to automatically request location information from the EISEC hub – this is civic address (including postcode) for fixed lines, and a location circle for mobile locations, of varying radius dependant on technology used to determine location (can be a less than 10 metre radius if satellite positioning available). This is covered in more detail in Supplier Information Note 278 - <https://www.btplc.com/SINet/SINs/pdf/278v2p4.pdf>.

Guidance on use of the location provided by EISEC is contained in Appendix 3.

If the caller remains anonymous the EA should request the customer identification details once the call has been terminated. Note this will not be possible in the case of emergency roamers.

Once connected to an EACR, the CHA EO will listen to establish that the caller is able to pass details to the EA call taker. Once the EO is satisfied that the caller is responding to the EA's questions, they will release the call from their position, to be held on the Operator Centre switch. However, if the EA's EISEC access is unavailable, and the caller is very young or very old, is panicking, is having difficulty speaking or where it is apparent that English is not the caller's first language, then the EO will normally listen throughout as it is very likely they will be asked for location information. If further 999/112 calls require answering, operators may make themselves available to answer the new calls, thus removing themselves from the listening process at an earlier stage.

**The extra digits, in addition to the caller's number, are to be phased out from mid/late 2020 to align with international standards and avoid issues with nuisance call management. The national organisation for the CHA and information from EISEC hub also means there is no need for the Operator Centre identity to be passed to EAs with each call.

7.1 EA REQUIRES FURTHER INFORMATION

If a caller clears before all relevant information is obtained, and the EA Controller does not end the call, the CHA will be alerted and an EO will return to the line for assistance. Calls are generally only released from the CHA when both parties using fixed lines clear.

If necessary, the EA can call the CHA Operator Centre national contact points using the agreed contact numbers - see Appendix 1. The EA will need to quote the time of the call, the caller's telephone number and whether the call was an emergency roamer.

If the call has not been released, the operator centre may then be able to associate the 999/112 call with the operator concerned who can then be advised to go back into circuit to speak further

with the EA. If the call has already been released, then the call records can be quickly consulted to confirm the basic call details.

The CHAs will hold call records for a period of three months. Call records include basic details such as callers telephone number, the time and date of the call, the EACR telephone number to which the call was connected and indications of any delay in connection or any unusual aspects of the call. For fixed calls the installation address will normally be present too. Note in the case of emergency roamers there will be no valid CLI for the caller.

Please note call recording access information is in **Section 13**

8. CALLS WITHOUT SERVICE REQUEST

There are many calls to 999/112 where a caller does not actually request an EA. In the overwhelming majority of cases these are children playing or customer misdials, but there is always a possibility of it being a genuine caller who cannot speak. In order to prevent the Police from being overwhelmed with these calls, the National Police Chiefs' Council (NPCC) have requested that the CHA operators filter such calls. To do so the CHAs use carefully designed procedures agreed with the NPCC.

8.1 CALLS WITHOUT SERVICE REQUEST FROM MOBILE PHONES

Very large numbers of accidental 999/112 calls are received from mobile phones. CHA EOs try to obtain a response by asking the normal questions – for example “which service is required”, and “if you cannot speak but need help please tap the handset screen, cough or make a noise.” In cases where there is:

- i. no speech and nothing apart from general noise is heard;
- ii. or where the voice link is terminated during CHA questioning, perhaps with background speech or noise;

It is recognised that there is a negligible chance that it is genuine and the CHA EO can end the call.

Where there is no response, the voice channel remains open and background voices are present, it is recognised that the CHA cannot decide whether an EA is needed. In this case the call is connected to a Police voice response system hosted by the Metropolitan Police Service which asks caller to press “5” twice if help is required. If 55 is pressed then immediate connection with the appropriate Police authority is made.

For any cases where suspicious noises are heard the CHA can override the above procedures and connect to a Police EACR.

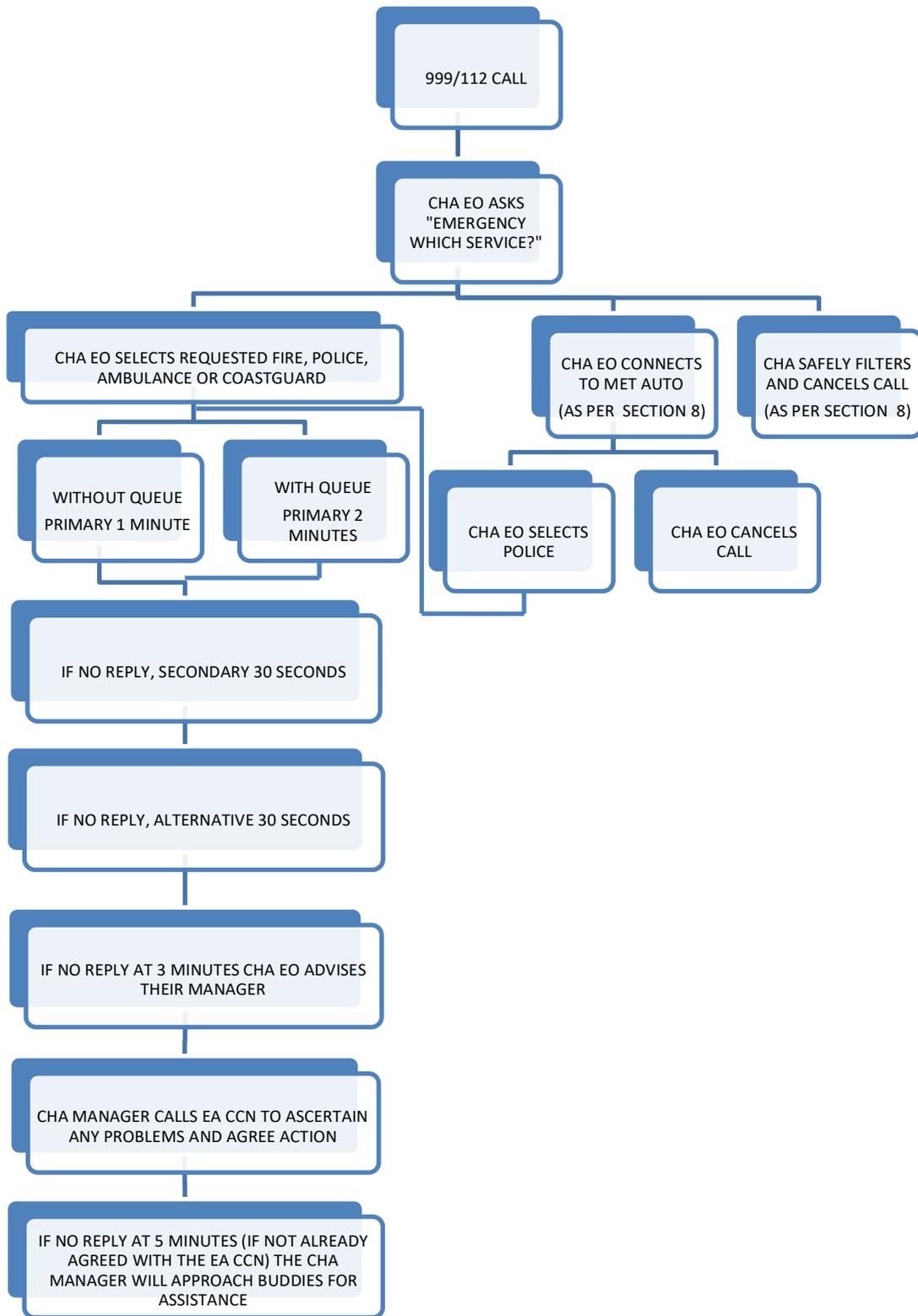
8.2 112 CALLS WITHOUT SERVICE REQUEST FROM FIXED PHONES

Switches on fixed networks still have to recognise loop/disconnect dialling and 112 calls can therefore be readily generated by faults within networks or customer equipment. Despite the use of network filters to prevent such calls reaching the CHA EOs, many are still received and appear as silent, open lines, or noisy lines with crackling and interference sounds. The overwhelming majority of callers on fixed networks use 999.

Once CHA EOs have asked their normal questions without response, it is agreed that there is an almost negligible risk of missing a genuine call. Therefore, for noisy 112 calls the CHA EO can end the call. Silent 112 calls will be connected to the Police voice response unit at New Scotland Yard. This provides one final check as described above to cover the rare case of a genuine 112 caller unable to speak being on the line.

For rare noisy calls to 112 on which the level of noise makes it impossible to listen, the call's voice link is cleared before details are passed to the Police by CHA EOs. This procedure will be kept under review in light of genuine use of the 112 code.

999 Call Connection Flow Chart



9. POST-CALL PROVISION OF CALL AND CALLER INFORMATION

9.1 PROCESS

The CHAs will pass information to the EA about the call and caller as the call is transferred to the EA.

If EISEC is used EAs can rapidly obtain fixed line installation addresses and approximate mobile locations for calling numbers by accessing the secure database that temporarily holds the details for 999/112 calls. Note: this information is not available if the call was made using a mobile phone in Limited Service State (refer to **Section 14**).

CHAs do endeavour to maintain a high degree of accuracy but are not able to guarantee the accuracy of the (fixed line) name and address information supplied verbally or via EISEC. CHAs do not accept any responsibility for the accuracy of the information provided to them by the CPs and have no liability for any injury, damage or loss caused by the provision of the information. Appendix 3 contains practical background and guidelines for the use of (fixed line) name and address information.

EA requests for information as described in this Section must be kept to a minimum, consistent with the essential nature of emergency call needs.

9.2 THE EMERGENCY PERIOD

The **'emergency period'** is defined as **within one hour of the termination of the emergency call**.

Within the emergency period the EA can re-contact the CHA and/or contact the relevant CP in order to:

- seek confirmation or reiteration of the call and location information
- obtain information about a caller (subscriber information)
- seek updated location information (if available).

A description of services and capabilities available at each CP can be found in the **'Dropped 999/112 and Disconnection procedures Crib sheet'** which is circulated to all Force Control Rooms on behalf of the 999 Liaison Committee

Specific guidance concerning the circumstances where data may be acquired or disclosed in relation to 999/112 calls is laid out in Chapter 10.5 of the Investigatory Powers Act 2016 Communications Data Code of Practice. See **Appendix 11** of this document.

As a rule, the acquisition and disclosure of communications data (subscriber information, call details and location information etc.) must only take place under an IPA authorisation or notice.

To enable the provision of emergency assistance in response to emergency calls which are 'dropped' or incomplete, Chapter 10.5 (Public Emergency Call Service 999/112 calls) allows an EA to call upon a CHA or relevant CP to disclose data about the maker of an emergency call within the emergency period outside the provisions of the Act (IPA). It goes on to say that in practice this means sufficient detail to identify the origin of the call and, if appropriate, to enable the deployment of an emergency service to the scene of an emergency.

After the emergency period an EA must contact an accredited IPA Single Point of Contact (SPoC) in order for the SPoC to follow their processes to submit an IPA authorisation or notice for the communications data required. In practice an EA could also be an IPA SPoC but the principal remains, outside of the emergency hour acquisition and disclosure of communications data must only take place under an IPA authorisation or notice.

An extract from the IPA (Acquisition and Disclosure of Communications Data) Code of Practice can be found at Appendix 11.

9.3 CONFIDENTIAL CUSTOMER INFORMATION

All caller and caller location information provided by the CHAs and CPs is strictly confidential and must be kept and used securely by the EA and only used for the purposes of dealing with emergency incidents. CHAs and CPs will authenticate EAs requesting information and will check the validity of requests.

9.4 MOBILE PHONE SUBSCRIBER CHECKS

Mobile phones making emergency calls could fall into one of a number of categories:

- a contract (or post-pay) account. Generally, these are accounts where customers pay for their mobile phone usage in arrears and are required to register (and have verified) their name, address and other contact details.
- a pre-pay account. These are accounts where usage is paid for in advance. Customers are not required to register their name, address and other contact details although some do. Registered contact details are generally not verified.
- a foreign roamer. These are (contract or pre-pay) customers from a mobile phone network operating in a foreign country which has a roaming agreement with one or more of the UK mobile phone networks. The UK network CPs do not have access to any subscriber information for these customers.
- a Limited Service State (LSS) roamer. These are (contract or pre-pay) customers who have no coverage from their home (UK) mobile phone network but are able to make 999/112 calls in LSS using another UK mobile phone network. See **Section 14** for further details.

9.5 MOBILE VIRTUAL NETWORK OPERATOR (MVNO)

These are sometimes called 'resellers' and operate 'virtual' mobile phone networks using some or all of the elements of the networks of the main four mobile phone CPs: EE, Three, Vodafone and O2.

Arrangements for the provision of MVNO subscriber information varies from MVNO to MVNO. Refer to **Dropped 999/112 and Disconnection processes** for further information.

Where a mobile subscriber is owned by an MVNO rather than the CP, it may be the responsibility of that MVNO to supply subscriber information. Where required an MVNO should ensure that it has a process to pass relevant subscriber information to an EA as required. This process should be available on a 24 hour basis.

10. MISROUTED CALLS AND MOBILE ZONE PROBLEMS

It is possible that the postcode, national calling number, zone code display or Cell ID could give an incorrect but apparently valid EA routing to the emergency operator. This could occur as a result of:

- i. a faulty console;
- ii. a fault in transmitting the information from the database;
- iii. more commonly, where a mobile handset has accessed a base station located in a different zone or Cell to the one where that handset is actually located. Handsets automatically search for the strongest signal and connect to the base station that they find provides it – this does occasionally mean it is not necessarily physically nearest to the site of the incident being reported. (This most typically will occur across river estuaries.)
- iv. where a call has originated from a private network that extends over several areas (DDI systems). In these cases, the number automatically presented to the CHA EO can be different to the number that the caller provides when asked by either the CHA or the EA. This is because any 999/112 call can be fed into the ECN in one of the areas. This can lead to problems as the CHA EO will be presented with a telephone number applicable to this area, and therefore routed accordingly. This will only become apparent at the EACR when the caller is questioned as to their location.
- v. where a call is an emergency roamer. In this case, a calling line number (CLI) may or may not appear but in any case, it will not correspond to the caller's number.

The CHA EO connects using the automatically presented information, as indicating the most appropriate EACR and to minimise any delay in connection. It is the responsibility of the EA controller to establish that the call is proper to the EA area and to instigate means of transfer if it is not. This can be achieved in a number of different ways in decreasing order of preference.

- i. Taking details of the call and passing the information to the correct EACR;

If option (i) is not possible, then

- ii. Recalling the CHA operator and requesting that the call is passed to another EA or County. This may not be possible if the CHA EO has already relinquished the call into the system.

If it is not possible for the EA to advise on the correct alternative EA or county, then the CHA EO will instigate a mobile call trace procedure as described in **Section 10.2** to identify where the mobile handset accessed the mobile network. The CHA EO will then re-route the mobile customer to the applicable EA control.

Note: Call traces can only be carried out providing the mobile customer continues to hold the connection.

The EA should not advise the caller to redial 999 and request a specific area or EA. The CHA EO will automatically connect the call to the relevant EA as per the presented routing information and override the request from the caller.

If a call has been misrouted the EA should advise the CHA by completing a misroute form found at Appendix 8.

10.1 BOUNDARY OVERLAP (Mobile ECNs)

Where cell or exchange coverage areas straddle two or more EA coverage areas, the CPs (or their call handling agents) will nominate an Emergency Authority Control Room (in consultation with the EAs as appropriate) to which 999/112 calls from that cell/exchange are to be directed. If this choice later turns out to be incorrect, the arrangements can be changed by mutual agreement. Comparison of exchange area/cell site boundaries and EA boundaries shows that exchange/cell boundaries are unlikely to overlap more than two adjacent EA coverage areas.

10.2 FAILURE TO DISPLAY ZONE OR CELL ID INFORMATION (Mobile ECNs)

Failure to display zone or Cell ID information is extremely unlikely. However, should this occur, the CHA EO will ask the caller for location information (e.g. county) and route the call accordingly.

If the location is not known, the CHA EO will tell the caller that there is a network fault and that some information checking will be necessary. The ECN will use inherent network facilities to locate the cell of origin. If the ECN is unable immediately to determine the zone code or Cell ID it will persist in determining the caller's location.

Note: It is recognised that extra time will be needed to go through this procedure.

It is essential that the ECN gives the CHA Operator a zone identity or Cell ID on all occasions and with the minimum of delay.

The cell and zone location facilities described above may be possible providing the calling mobile holds the connection. If the caller clears, traces are not generally possible, but records are kept by the CPs which include time of call, duration, originating number, the cell which received the call and the resulting zone code (where applicable). These records are kept and will be readily available for cross-checking for approximately three months. Note in the case of emergency roamers, the data will be restricted to time, duration, the Cell Id and the IMSI number which identifies the SIM used and records may not be kept in these cases.

11. ROUTING METHODS AND FAULT MANAGEMENT

11.1 ROUTING METHODS AND NETWORK SECURITY

In the digital network, the standard method of routing 999/112 calls from CHA EOs to EACRs will be via each PSTN (though not for the majority of FRS connections). Calls will normally be connected over the primary route to the nominated EACR. The digital network provides good transmission and fast call set-up. It also provides forwarded 999/112 calls with automatic alternative routing through the network to the nominated EACR, along with priority treatment over normal calls which particularly helps on occasions when the network is busy. This method of routing provides sufficient resilience to meet the obligations under the General Conditions of Entitlement.

All mobile CPs will provide capacity from their Mobile Switching Centres ("MSCs") to enable calls to be routed to the appropriate first choice operator centre. The capacity provided will be secured by supplying diverse transmission routes, where possible, to minimise the effect of equipment or line plant failures.

Alternative routings from the MSCs will be automatically invoked when route congestion to, or failure at, a switch is detected. Note: Any circuit suspected of being faulty will be removed from service until such time as engineering tests have proved the fault rectified and operational tests have been performed.

Further safeguards exist in the form of a back-up service provided between the Operator Centre switches which will be effective against temporary closure of the Operator Centre site due to emergencies such as fire alarms or bomb threats. BT's CHA currently has 6 OC sites and 3 separate switch sites.

11.2 PRIORITY FAULT REPAIR SERVICE

EACRs need to make clear to the CPs that provide their 999/112 service that priority should be given to maintaining service to all 999/112 circuits in accordance with the relevant regulations.

Condition A3 of Ofcom's General Conditions of Entitlement states that all CPs must take all necessary measures to ensure uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered. This will involve the protection of the physical and functional operation of such systems and services against malfunctions or failure caused by electrical conditions, signalling protocols or call volumes.

11.3 ISOLATION OF CUSTOMERS DUE TO NETWORK FAILURE

In the event of a major failure to a part of an ECN, the CP will notify the affected EAs as soon as possible after the failure is identified or anticipated. CHAs and CPs will assist the EAs in order to overcome the situation. A copy of the BT CP process has been circulated to all EA contacts. Further copies can be issued on request, for contact details see Appendix 1.

EAs and relevant CHAs should adopt local contingency arrangements for 999/112 call handling in the event of a network failure. EAs should prepare contingency plans to cover lack of network access to 999 through their Local Resilience Forums.

11.4 DRAFT MEDIA STATEMENT FOR CHAs/CPs AND EAs

The decision on whether to inform the public and what to tell them is not straightforward but may need to be given for any significant failures lasting an appreciable length of time. A CP/CHA should try to help by giving estimated times for the full service to be restored and by advising whether the failure in a given area is affecting all their lines or a scattered distribution across the area. Mobile telephones are widely available and more than one company may provide fixed telephones in an area, therefore, the loss of one ECN is not always critical.

When a network failure is judged to require a statement to be issued to the media, the following sentences should be considered. **The statement should be jointly agreed and issued by the CP/CHA and EAs concerned** with the affected area. It can be modified where appropriate, for example those areas in italics need to be considered for each incident.

- (CP/CHA name) have notified us of problems affecting telephone service in the xxx area.
- They are currently working to restore *full* service to everyone as soon as possible.
- You can also try dialling 999 from a mobile phone, if you have access to one, since the mobile phone networks may still be working normally. If your mobile network is not operational, you may still be able to make an emergency call via another mobile network by calling 999 or 112.
- We are asking people not to make any non-urgent calls for the time being so that all the available phone lines can be used for real emergencies.
- Even then, some people may be unable to use their own phones, or public payphones, to call the 999 emergency services. You might be able to call your nearest police station directly or 101 even if the 999 service has been affected.
- Extra police patrols are out on the streets, so if you need help and are able to get out, try to get the attention of a police officer or a passing police car.
- You could also seek help by going to your nearest police station, hospital, fire or ambulance station in person.
- We will give you an update on the situation as soon as we have more information.

Social media messages

For significant outages lasting an appreciable amount of time it may be appropriate to post an update via social media. Again, this should be agreed with or advised to the CP that the post is being made. A suggested post is below.

You may face problems calling 999 from a landline in the xxx area, try calling from a mobile phone as mobile networks *may be/are* working normally. Normal service will be restored ASAP.

A follow up status message should be provided as soon as there is an update or when an issue is closed.

12. MANAGEMENT OF MAJOR INFLUXES OF EMERGENCY CALLS

12.1 ADVANCE WARNING OF MAJOR INCIDENTS

In some cases, prior warning of major incidents are possible. Extreme weather, special events such as the World Cup, and Christmas / New Year social activity are all well-known sources of additional 999 calls and are known about in advance.

All EAs and CHAs need to assess the Impact of Weather Forecasts available from the Met Office and the Environment Agency/ Scottish Environment Protection Agency.

Staffing arrangements for both EA and CHA control rooms should be adjusted accordingly in the light of these forecasts and known impacts from previous similar events. CHAs and EAs should exchange information on predicted impact on the 999 service of predicted events, for example the volumes/times of increased 999 demand. In particular an EA should notify the CHAs as soon as possible if a likely staffing shortage is identified that could affect handling of 999s.

The use of media announcements should be considered by EAs in order to minimise public reliance on the 999 system. Advice could be given about preparations already in hand for their area, what will be considered an emergency, where to seek further guidance or assistance etc

12.2 CONTACTS

EAs should check with CHAs to ensure they hold the correct “buddy” arrangements, offering additional buddies if necessary e.g. more distant ones likely to be unaffected by the event. Agreement should be confirmed between buddy EAs on how information will be passed e.g. fax, email, electronic interfaces, CAD/Command and Control logs, radio, DEIT, MAIT, or dedicated voice channels etc.

Consideration should also be given to the use of non-emergency numbers (such as 111 or 101) where appropriate.

Conference Calls should be considered where ongoing contacts are going to be needed during a major incident and if many parties are going to be involved at the same time. These can be established between EAs and CHAs or simply among EAs with feedback/instruction for the CHAs. Such Conference Calls should follow an established process and can be part of any Silver Command structure established to manage an event or established specifically to manage 999 call handling issues.

Note: To establish a Conference Call an invitation and standard agenda is available in Appendix 5. This will be issued by the CHA using 24-hour contact points within EACRs, usually for the affected EAs and their buddy EAs.

12.3 MODIFICATIONS TO QUEUEING SYSTEMS

See **Section 6** for general use of queues. If possible, and the queuing system allows, extra information can be temporarily inserted into the announcement to try to manage demand and caller expectations. For example: “.....We are currently receiving a high volume of calls due to (major incident details).”

12.4 CHANGES TO CALL HANDLING PROCEDURES

12.4.1 GENERAL STEPS

- It is important that EAs and CHAs establish contact with each other as soon as possible after a major incident/event has been identified that is affecting 999. This may be before the impact is fully assessed.
- The EA will contact the CHA to advise of the impact they are expecting/experiencing and give revised call connection instructions if a change is required.
- The CHA will contact the EA if the EA's time to answer is exceeding 3 minutes (i.e. when neighbouring services would already be assisting on multiple calls).
- In such circumstances the phrases below would normally be agreed between the EA and CHA for the duration of the incident/event in question.
- If contact is not quickly possible, so as to protect calls to other services, the CHAs would move automatically to these expressions as soon as (a) delays of greater than 3 minutes in connection to one or more EAs are sustained for more than 15 minutes, or (b) the delays are such that they severely affect the CHA's own ability to answer 999 calls quickly for more than 15 minutes.

Expression: "(EA name) is very busy with calls relating to (major incident details) at (location). I will try to connect you."

12.4.2 FLOODING INCIDENTS

- If specifically requested by a Fire Service trying to prioritise many flood-related calls and allow normal fire service calls to be answered, the CHA may agree to ask further simple questions before connection, in an effort to filter-out non-emergency cases on behalf of the EA.
- First question would be: "Are you reporting a flood ?"
- If not a flooding incident, the CHA would connect straightaway as normal. If a flood, a further question would be asked: "Is anyone in danger?" If the answer was "yes", or doubt existed, or the caller insists on connection, then the call would be connected to the Fire Service as normal. If not, the caller would be told "XXXX Fire Service is very busy with flood related incidents. If the situation becomes worse, please call back."
- This instruction from the Fire Service would need written confirmation (email or fax) from the Fire Service to the CHA to back-up a verbal instruction.
- If contact from the Fire Service is not quickly possible, so as to protect calls to other services, the CHA's would move automatically to these expressions as soon as
 - a) Delays of greater than 3 minutes in connection to one or more EA's are sustained for more than 15 minutes, or
 - b) The delays are such that they severely affect the CHA's own ability to answer 999 calls quickly for more than 15 minutes.

12.5 MEDIA ANNOUNCEMENTS DURING A MAJOR INCIDENT

All parties should refer to the guidance notes and follow the correct consultation process before releasing any statements to the media. See **Section 11.4**

Draft Press Release:

Press Release on behalf of the emergency services in (county) in partnership with the 999 Call Handling Agents British Telecom

The emergency services in (county or location) are currently experiencing a high demand of 999 calls due to

The emergency services and the 999 call handling agents are doing all they can to respond to this unusually high level of demand.

We would appeal to the public to consider whether or not it is necessary to dial 999.

If their call is an emergency, for example, any life-threatening situation, a fire, or a crime in progress, they should continue to call 999. But we would like to remind them that if their call is for a non-emergency situation there are alternatives to the 999 system, these are:

Police:

Fire and Rescue Service:

Ambulance Service:

Please listen to local radio stations for further information.

Note to Editors etc:

Enquiries about this News Release should be made to:

13. RECORDING OF CALLS

CHAs will record all calls terminating on 999/112 circuits. Calls are recorded from the time at which they are presented to the emergency operator until the caller clears and the circuit is released, regardless of whether the CHA has monitored throughout. The original 999/112 recording tapes are kept by CHA's for a period of 3 months (93 days).

Access to recordings of emergency calls can be gained for investigatory purposes where it is required as evidence or similar use. Evidential quality copies can be requested if necessary. Requests from EAs to listen to or be given a copy of a recording of a 999/112 call must be referred to the agreed contact point within the CHA.

To access a recording from BT, a Court Order or Customer and EA consent is required. This should be sent via the Single Point of Contact (SPoC) who would then send the request to the address listed on Appendix 1. SPoCs should be contacted first for advice and guidance.

The following levels of authority are required for access to be given:

Police – Assistant Chief Constable
Fire – Assistant Chief Officer
Ambulance - Director of Operations
Coastguard – Chief Coastguard

CHAs should apply to the Chief Officer of the relevant EA for similar recordings of calls made by the EAs.

All CHAs inform their customers that they should use the 999/112 number when making emergency calls. CHAs do not tape record emergency calls made on 100 circuits (general operator services access code) when a caller inadvertently uses the 100 code. However, such calls are handled despite the use of the incorrect code.

14. OTHER TYPES OF CALLS

Other types of call may include:

- Limited Service State
- Text Relay
- eSMS
- Telematics
- Other Vehicle Activations

14.1 LIMITED SERVICE STATE EMERGENCY CALLS

This section contains details of 999 or 112 emergency calls made from mobile telephones which do not have network coverage from their own provider. These calls are referred to within the Mobile CPs as “limited service state” but the emergency services may refer to them as Emergency Roamers, displaced or camped calls.

Background

During the latter part of 2008 the EU advised Ofcom that the UK was the only EU Member State that did not provide the ability for users to make 999 or 112 on another network. Ofcom therefore required all UK CPs to make this facility available to users – thereby allowing users to make such calls when out of the coverage of their home network and thereby maximise the ability for users to obtain help quickly. This functionality should not be confused with foreign mobiles visiting the UK as roaming agreements would be in force that would allow the user to make and receive calls as normal.

Considerations for the emergency services

Whilst Limited Service State has the benefit of allowing users to dial 999 when outside of their home network coverage, it does present challenges for the emergency services. It is important to note that these types of calls will not contain all of the data normally associated with a conventional emergency call and there will be limitations with regard to locating where the call was made from.

- The call will present to the CHA operator with either no telephone number (CLI) or a default number. Either way the caller’s own mobile number will not be presented.
- Location for these calls is confined to either the Zone code or in some cases the Cell ID. These codes are used to route calls to BT and the emergency services only and therefore do not provide any assistance to identify the caller’s location.
- The CHA may be able to pass the caller’s telephone number verbally if the caller relays it while waiting for the EA to answer
- The CHA will advise the EA that the call is a “Limited Service State” call. The CHA process involves a verbal handover and will change from announcing as emergency roamer to Limited Service State during 2014 to align with industry terminology.
- If contact with the caller is lost, it will not be possible for the CHA or EA to contact the caller even if the mobile number has been obtained UNLESS the caller has moved and is now within coverage of their home network.
- If the call drops, the EO would normally contact the CHA to gather additional information. In such circumstances, the EO should advise the CHA that the call is a Limited Service state call. This will alert the CHA to the processes they have in place to assist with trying to trace such calls. (The EO should quote Limited Service State

caller together with the date, time, number which was displayed on EISEC and the customer telephone number (if it was obtained.)

- It may be possible for MNOs to provide additional information. However, this could, in some circumstances take up to two days due to the technical challenges locating such a call although this will vary between networks. It is generally not possible for any of the MNOs to provide “real time” information within the golden hour.
- A mobile telephone number will not be available to the MNO who carried the call. The only information that will be presented to the MNO is likely to be the IMSI. Further work would therefore be required by the EA to identify the “home” network in order to acquire subscriber details.

A disadvantage of Limited Service State is that users can make hoax calls to the Emergency Services on another network to their own even if the user has been disconnected from their home network. EAs should therefore be aware that requesting users to be disconnected for making hoax calls does NOT prevent them from making further calls as calls can continue as a Limited State Service call. This therefore makes the situation worse as the mobile number will no longer be presented at the time of the call.

As mentioned above, it may be possible for MNOs to provide additional information which would assist in identifying the caller but such an activity cannot be performed in real time and would require an IPA request to be issued to the MNO.

14.2 TEXT RELAY (Previously Text Direct/Typetalk)

The Text Relay service is used by customers who are deaf, hard of hearing, deaf-blind, or speech-impaired and use a text phone to make or receive telephone calls. BT provides a unique code for Text Relay customers to make emergency calls and this is 18000.

The Textphone

Customers who cannot use voice will use a textphone to make and receive telephone calls. A textphone can be thought of as a standard telephone but with the handset replaced by a keyboard and display. Two textphones can communicate over a standard telephone call. The characters that are typed on the keyboard of one textphone are transmitted to the other textphone as tones in real-time i.e. each character is sent as it is typed and the user does not have to press Enter to send the text. This of course only works if both customers have textphones. If one party does not have one, then the call has to be facilitated by the Text Relay service.

Text Relay

Text Relay is a network-based service that BT provides to support customers who need to use textphones. Any customer making a textphone call, or wishing to communicate with a textphone user, will use Text Relay. There is no registration required; all the caller has to do is dial 18000 and the 18000 calls initially terminate on one of four Next Generation Text (NGT) Service nodes. The call will be answered by a 999-emergency advisor (EO) who will be joined at the same time by a Text Relay Assistant. The Relay Assistant will translate the conversation by reading the typed text from the textphone user to the voice user (EO) and typing their spoken reply. They should not add or subtract anything from the conversation, and they have no control over the call. Customers using the service can be connected in either text or voice to 18000.

The BT 999 Advisor will announce to the emergency services that the call is from a text user. It is possible to receive the calls from mobile phones but in these circumstances the customer will be connected in voice.

If the call is made from a BT customer, name and address details will be provided however, this may not be the case for customers of other CPs.

If for any reason the Text Relay service is extremely busy a call may arrive with the BT 999 Advisor without the Text Relay Assistant in conference.

NOTE: There is also the Next Generation Text (NGT) App that enables users to type and read over a separate data link via the internet to the NGT nodes in parallel with an 18000-voice call. When using the NGT App the caller can simultaneously type, read, speak, or hear depending on their individual communication needs. The Next Generation Text Relay was launched in 2014, incorporates the text relay service, and can now be accessed on a range of mainstream devices, including smartphones, via the free App. See www.ngts.org.uk for details.

14.3 eSMS

Guidelines for the eSMS service were established by the UK Government's 999 Liaison Committee and an MoU was drawn up to set out the service parameters, a copy of which can be found as **Annex 1** to this document (embedded document).

The SMS Emergency (e-SMS) service is provided for people who are deaf, hard of hearing or speech impaired as an alternative option for contacting the EAs as they may experience difficulties in using the voice 999/112 service. The overall objective is to provide a customer experience as similar to that of the voice 999/112 access as possible.

An e-SMS can be sent from a standard mobile handset, but end-users will be required to be registered for their text to be recognised. When an e-SMS is received, the originating phone number is checked to ensure that it is registered with the service, before it is translated and passed on to Text Relay. An e-SMS from an unregistered phone number will be rejected and sent an automated message advising that the user is not registered and needs to contact the emergency services using other methods.

Caller Location information is made available from the originating network and provided to the EA in the same way used for voice emergency calls. The CHA will set-up the voice call as soon as technically feasible after the requested EA is known, and to the Police if no EA is requested.

An outgoing PSTN emergency voice call will be generated using the e-SMS originating phone number and will get directed to the designated 999 Call Handling Service. Responses from the 999 Service operator or EA operator conveyed by the Text Relay assistant will be converted into an SMS by the e-SMS service and sent back to the originating mobile phone number.

Follow up arrangements for EAs on calls will be through the same contact points as for emergency voice calls.

14.4 eCall AND TELEMATICS EMERGENCY CALLS

eCall based on 112 is a mandated system (with Telecommunications Regulation and Vehicle Type Approval rules) that provides an automated message to the emergency services following a road crash which includes the precise crash location. The in-vehicle eCall is an emergency call (an E112 wireless call) generated either manually by the vehicle occupants by pushing a button or automatically via activation of in-vehicle sensors after a crash. When activated, the in-vehicle eCall device will establish an emergency call carrying both voice and data (using a modem) directly to the designated 112/999 Public Safety Answering Point, PSAP. The voice call enables vehicle occupants to communicate with the trained eCall operator. At the same time, a minimum set of data will be sent to the eCall operator receiving the voice call. The minimum set of data contains information about the incident including time, precise location, vehicle identification, eCall status (as a minimum, indication if eCall has been manually or automatically triggered) and information about a possible service provider.

Telematics is a service where mobile phone technology in a vehicle is linked with position information derived from satellites. The service pre-dates eCall and uses an SMS or mobile data message to transmit vehicle and location data prior to setting up a voice call to a specified number (not an emergency number in same sense as eCall).

The CHA EO (designated PSAP) will connect call to the appropriate EA in the normal manner but highlight that the call is a “Telematics mobile” or “eCall mobile” and add GPS location information or, if there is a delay in receipt of location, will interrupt with location details when available. The map reference is a fully numeric 14 figure Ordnance Survey grid reference. Satellite positioning of the eCall system now provides an accuracy of +/- 15 metre from the final location provided. The CHA EO is able to do this as in addition to receiving the voice call they will also receive data containing the vehicle and location details from a modem transmission at start of voice call (for eCall) or via a separate data message (for Telematics calls). The location data and vehicle data is provided to EAs over EISEC. This type of call normally includes voice and data, however, on occasion the CHA EO may receive a voice only call or a data only call.

The EA operator is then able to directly question the caller as normal.

If the caller is unable to supply the needed information, and it is not present on EISEC, the EA operator can ask the EO for further details and usually obtain direction of travel (N, NW, W, etc or degrees), make, model, colour and registration of vehicle or VIN number, and sometimes other personal information supplied by the customer.

Emergency roamer calls cannot be made over the Telematics Service. The service requires connection to the home network to function.

The full Telematics Protocol for handling eCalls and Telematics emergency calls can be found at **Annex 2** (embedded document).

14.5 OTHER VEHICLE ACTIVATIONS

Ford has an in-car system which allows the customer's mobile phone to be connected to an in-car monitoring system. In the event that the car is involved in a crash where the air-bag is deployed or the fuel pump has been cut off, the car will make an emergency call from the customer's mobile. This system has now been superseded by the mandatory introduction of eCall based on 112. When the CHA answers the call the in-car system will play a message to the EO giving the co-ordinates of where the caller is. If the call is silent, or there are problems obtaining location from the caller, the call playback facility can be used to allow the co-ordinates to be played directly to the EA operator.

Vehicle emergency activations using 3rd party call Centre

Some car manufacturers have chosen to have their in-car emergency call activations (eCall and Telematics) answered by a call centre, which can be located in the UK or elsewhere. The call centre will establish if the customer requires emergency assistance in the UK and if so, they will connect the customer to the CHA in the UK. The third-party call centre will ask for the emergency service type required and pass all relevant information including the location and vehicle details prior to opening a conference so that the EO can speak directly to the customer. The data generated by the vehicle can be passed verbally or by electronic transfer.

15. NUISANCE AND HOAX CALLS

Hoax calls are made to the emergency services by individuals who deliberately report an emergency when one doesn't exist. Hoax calls divert the emergency services away from people who may be in life-threatening situations and who need urgent help.

Whilst **nuisance calls** may be deliberate, they are generally not made maliciously and may happen for a variety of reasons; it could be children playing with a phone, a person might be lonely or vulnerable or perhaps has mental health problems. These callers may not necessarily be calling the emergency services for urgent assistance and may not understand that their actions are not acceptable. Consideration should be given into how best to deal with such callers to ensure that their access to the emergency services is not interrupted or harmed in any way in the event of a genuine emergency.

Whatever the case, the making of **hoax** and/or **nuisance calls** to the emergency service is a criminal offence under the Communications Act and breaks the terms and conditions of a caller's contract with their mobile phone provider.

For persistent hoax callers the primary objective should be to identify and prosecute offenders. Mobile Network Operator (MNO) retain useful information that can assist in this objective. Many hoax calls are made from mobile phones with pre-pay SIMs for which subscriber information may not be available (or if available, may not have been verified). There are, however, a number of investigatory methods that may be employed to identify the user, but this is only possible whilst the user is connected to their home network. Also, to be considered is the availability of widely available free pre-pay SIMs. As one account is disconnected so a hoax caller could simply resume making calls using another SIM and any investigation must start from scratch. Contact should be made with an IPA Single Point of Contact (SPoC) who will advise as to what data might be available and how to obtain it. All police forces have an IPA SPoC that should be consulted if an emergency authority does not have an IPA SPoC of its own.

Many MNOs proactively monitor hoax/nuisance emergency calls and have processes in place to contact customers to educate them about the impact their behaviour has and to insist that the customer desist from the behaviour. In most cases this appears to discourage hoax/nuisance calls and an emergency authority should consider requesting that an MNO contact their customer to try this approach.

Although not recommended (as the investigatory opportunities described above are degraded), an emergency authority can request that an MNO disconnect the account of the hoax/nuisance caller. However, a disconnection will not stop emergency calls from being made as they will still be possible in 'Limited Service State (LSS). LSS enables customers to make emergency calls even when outside of the coverage of their home network. This is of course very valuable in the terms of access to the emergency services when a person has no coverage from their home network but does pose a problem in tackling hoax/nuisance call. When calls to the emergency services are made in LSS the calling number is not presented and information about the call and the caller held by the MNO is of little use (see Section 14 for further details).

An emergency authority must submit a disconnection request to an MNO using the request form at Appendix 6. The MNO will normally insist that at least 3 hoax/nuisance emergency calls have taken place and will verify this by checking call records. The form must be authorised by a police inspector, watch manager or equivalent, accepting the risks set out in

the form. An MNO may refuse the request in favour of their own process to contact the customer as described above.

Hoax VoIP calls – see Appendix 9

APPENDIX 1: CHA CONTACT DETAILS

	Contact	Telephone	Email
For notification of <ul style="list-style-type: none"> • Misroutes, • Problem reports • System outages • Changes to emergency telephone numbers • Boundary issues • Enquiries related to BT Emergency Operator Services 	BT 999 Liaison Team	0800 1697 999	999liaison@bt.com
Urgent out of hours contact with BT 999 Centres	Glasgow or if unavailable Bangor or Dundee	01633 212032 0131 3001999	
Names and address enquiries within 60 minutes of the 999 call	Glasgow	0141 2485813	
EE subscriber checks within 60 minutes of the 999 call	Nottingham First choice If not answered within 2 minutes, please try alternative	0870 2400323 01159 241133	
<ul style="list-style-type: none"> • Name and address enquiries, (including those made longer than 60 minutes after a 999 call) • Access to call recordings 	BT Group Engineering Services pp A6G, BT Centre 81 Newgate Street, London EC1A 7AJ	0845 2661761	
Process queries for the Loss of Access to BT Public 112/999 Service	Civil Resilience		emergencyplanning@bt.com
Contact for Hoax Calls	BT Nuisance Calls Bureau Monday – Friday 08.30 – 17.00	0800 411422	

APPENDIX 2: MOBILE NETWORK OPERATOR CONTACT DETAILS

Mobile Network Operators' contact details and processes for EAs are available in the Dropped 999/112 and Disconnection process Crib Sheets distributed separately.

APPENDIX 3: GUIDANCE ON USE OF LOCATION INFORMATION

Although CHAs endeavour to ensure data accuracy they cannot claim 100% accuracy for the address information which is supplied to them by the CPs serving the end-users. Experience over the years with addresses supplied verbally by operators, and now automatically by EISEC or similar systems, shows a high degree of accuracy is maintained on the CHA databases.

The following guidelines will help call takers/despatchers when working with caller name and address information.

EA Call taker /despatcher guidelines

1 Fixed Lines

In the first instance the EACR call-taker can have a high degree of confidence in the accuracy of the CHA-provided address. The rate of critical errors found in this data is typically much less than 1 in 10,000.

There are known instances where the address provided by the customer may well differ from that provided by the CHA. In these known cases, the CHA will provide indicators with the data to show that the address provided may not be accurate. These situations arise because of the communications technology the caller is using:

1.1 Private Networks

Many businesses have private networks known as Private Branch Exchanges (PBXs). Historically, for example a company could have a published main number of 0113 237 6400 with 30 lines that can be used for incoming and outgoing calls for the 200 employees, each with their own extension. External customers dial the main number and are connected to the required extension by a switchboard operator. Outgoing calls go automatically through the switchboard, usually by dialling a network access code such as "9".

Modern PBXs provide Direct Dial In (DDI) facilities, which for this example may lead to the company in this example having 200 incoming numbers (e.g. 0113 237 6400 to 0113 237 6599), all accessible directly to external callers. However outgoing calls still use the main number 0113 237 6400. This is the number displayed to the CHA's agents and passed to EACRs. The address automatically presented to an EACR is the one held by the CHA that is associated with this main switchboard number. Since some companies spread their DDI extensions over a number of sites, or across a large site, the caller may give significantly different address details to those supplied by the CHA as well as passing their own DDI number which will be different from the presented, main number. Such PBX/DDI addresses are marked with ****EXT**** at the front of the name to show that the caller may well not be at the main address but that of an extension on a different site.

Even if the EACR calls the CHA to check address details for the customer-passed DDI number, the CHA's records will only show the address of the main switchboard, as customers do not in the main provide their CPs (and hence the CHAs) with addresses for individual extension numbers. The only way to check a caller-passed location on such a call is to recall the DDI extension or main number and enquire of the customer or their switchboard staff respectively.

1.2 VoIP – Voice over Internet Protocol - calls

An increasing number of customers are using VoIP devices (telephones or PCs) to make calls – often over broadband internet connections. For VoIP calls the telephone number (or calling line identity, CLI) is not directly linked to the line being used, but rather to the user or terminal. Customers of some services can simply unplug their telephone from the Internet (or their corporate intranet) and reconnect at a new location that allows access to their VoIP Service Provider, and they will keep the same CLI. Similarly, a PC user can register themselves onto the Internet anywhere (e.g. using publicly available Wi-Fi connections) and make and receive calls with the same CLI.

At present most users will be at one fixed location – their home or default location - and the address provided for their CLI will be this default address. To assist EACRs the address will be marked with ****EXT**** at the front of the name to warn that the caller may not be at the address given. There are also VoIP Service Providers that do not allocate individual CLIs to every registered user; this may be because the Service Provider provides some of their customers with an outgoing calls only service where it is not possible to call the user back, for example some of SKYPE's customers. In these cases, a default, non-geographic CLI is presented on all emergency calls.

Currently it is not technically feasible to provide accurate location details for VoIP users other than the default address; however it may be possible for the Service Providers to trace the originating IP address and block hoax callers, or provide the registered user's contact details.

1.3 There are other reasons when the address provided by the caller may not match that provided by the CHA:

(i) The caller has recently moved address

Name and address details are updated as necessary between once and up to four times a day depending on the CP. There are thousands of updates made each day involving new customers taking out service or existing customers moving address and taking their telephone number with them. The names and addresses provided by the CHA for these numbers will be incorrect for about half a day and is a known source of discrepancies between reality and data the CHA holds, occurring in about 1 in 10,000 calls.

(ii) The caller is using a re-sold line

The name that appears in the name and address details may not be that of the caller. An increasing number of BT maintained lines are rented in bulk by CPs that then provide telephone services to individual customers. In such cases it is sometimes the CP name that is provided though the address is that of the individual customer. Most instances of this issue have been tackled and CPs are working to replace the CP name with that of the end-user name.

(iii) The caller is reporting someone else's emergency

There are instances where an emergency incident is reported by a third party and where the address they report may not match that held by the CHA.

Alarm monitoring companies provide a commercial service to care homes, other businesses and individuals. They will receive a call from a client and then contact the EACR on their behalf. The telephone number they quote to the CHA as being that of the original caller and the address they provide, possibly from a confused caller or from their own database, are subject to increased errors.

Neighbours and bystanders can provide address information for affected premises which they think is correct but may well not be and which will not relate to the telephone number of the person making the call

Non-emergency services such as 101 or 111 may take calls which then need escalating to a 999/112 call. The call will usually present to the EACR in the same way as that from an alarm monitoring centre

2 Mobile Calls

EACR need to ensure the full EISEC specification** is supported by suppliers of their control room systems – this allows both an approximate network location and a more precise handset location where available (known as Advanced Mobile Location, AML) to be retrieved through the EISEC interface (separated by a short time delay to allow handset to fix its location). It also allows retrieval of location and vehicle details for eCalls and Telematics calls.

** See Supplier Information Note 278 for more details - <https://www.btplc.com/SINet/SINs/pdf/278v2p4.pdf>

EACRs need to display full location information on a call taker's mapping screen – this will be a location circle of varying radius for mobile callers (showing both a network location and a handset location where possible), and not simply a point as seen for fixed line addresses. The diagram below illustrates this, showing the differing precision of network and handset locations. There will also be a Level of Confidence value that caller is within the circle that should be displayed.

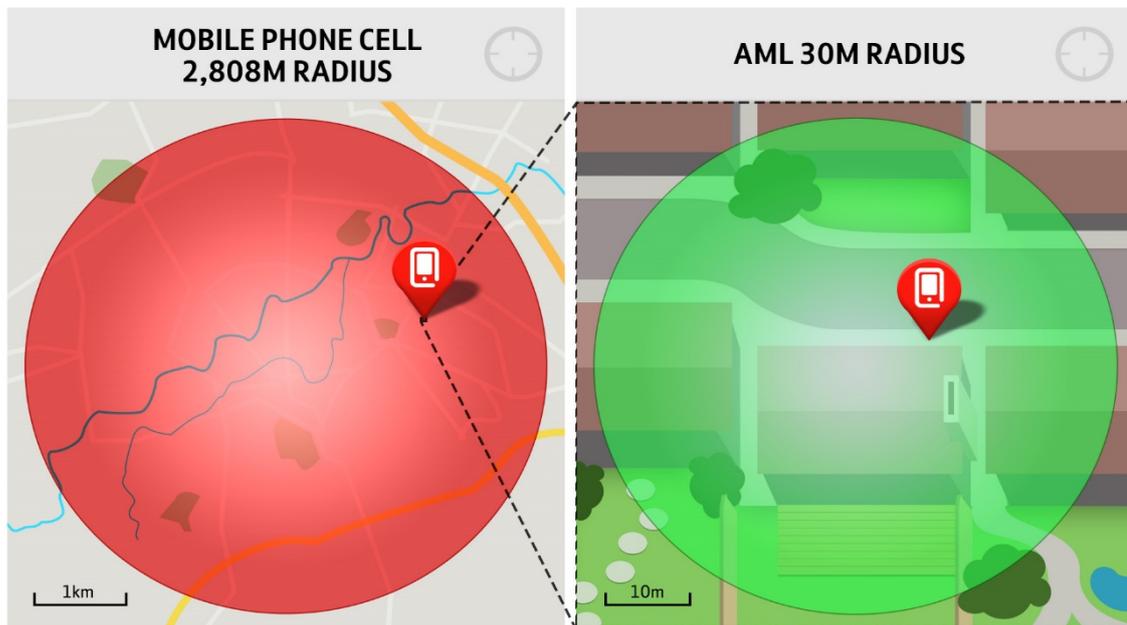
In addition, command and control software needs to be able to use the mobile location which is provided using a map reference, not a civic address with a postcode.

EACRs should ensure that call handling systems allow call takers to match the coordinates provided as part of the handset locations to (a) nearby locations used within local databases that can be relayed verbally if needed, or (b) matched directly to responding resources with a free text description added if more appropriate, e.g. '100 metres west of {Nearest Property, or Road Junction, as matched by local address database}'.

There are some cases where no network location can be provided – this is the case with Limited Service State calls (also known as emergency roamers) where a handset has no coverage from its home network but can use another network, or from overseas users in the UK roaming onto UK networks. AML is also not available from Limited Service State calls.

Handset Location (AML) is available from most smartphones, but is not always technically feasible (e.g. if no access to satellite positioning), or possible from other handsets without a smartphone capability. At the time of this update (October 2018) it is present for almost 70% of mobile emergency calls.

AML (Advanced Mobile Location) suburban location



3 When things go wrong

3.1 For fixed lines

Despite the data integrity checks carried out and the annual audit of the data held by the CHAs, things can go wrong and the address provided by the CHA for a 999/112 call can be incorrect.

If the EACR call-taker has reason to doubt the address provided by the CHA (from what the caller has said) then they can recall the Operator Centre in the normal manner and ask for the address to be checked. The CHA will then check their own database and if necessary, will either contact the serving CP to confirm the caller's address or will provide the EACR with a contact point in the CP that the EACR can deal with directly.

Any discrepancies found when using EISEC or similar systems should be e-mailed to the CHA's data discrepancy team in accordance with the detailed procedures provided by the CHA. Form found in Appendix 8b.

3.2 For mobile calls

A network or handset location is sometimes not possible due to technical limitations or systems issues, and there can be occasional errors in network or handset information used to derive locations. Verbal confirmation with callers wherever possible, as well as comparing network and handset locations, helps to quickly identify any such issues.

APPENDIX 4: BEST PRACTICE GUIDE FOR CPs ON NAME & ADDRESS INFORMATION (LANDLINES)

This set of guidelines has been developed through discussions with Ofcom to help ensure Communication Providers (CPs) achieve compliance with the General Conditions of Entitlement (GC 4.2). They provide reassurance for the Emergency Authorities on the efforts made to ensure that address information supplied to them by the CHA on each 999/112 call is as correct as practically possible.

1. The Communication Provider (CP) will be expected to ensure that the location information provided to the Call Handling Agent (CHA) is correct and up to date. The CP shall take steps to ensure that installation addresses are not confused with billing (or other) addresses related to the end user.
2. New location information and routine updates to location information should be notified to the CHA by the CP within one working day of the new, or changed, line termination arrangements being completed. With regard to ported lines, both the gaining and losing CPs need to comply with this recommendation to ensure the integrity of the data held by the CHA
3. The CP should ensure that addresses supplied are validated by reference to a recent (not older than 6 months) version of the Postcode Address File (PAF) and that it also conforms to the data structure required by the CHA.
4. The CP should ensure that the CHA is notified of newly activated, or re-assigned, number ranges before records of CLIs and addresses for those CLIs are sent to the CHA. Failure to do so will delay the loading of the data onto the CHA's database as the CHA carried out further data integrity checks
5. The CP should, at a minimum, conduct an annual audit to compare names and installation addresses held on the CP's own systems with the location information held on the CHA database. Ad hoc audits may be required in cases where the level of discrepancies for a CP begins to give cause for concern or where significant system changes have taken place.
6. The CHA will normally inform the CP of any discrepancies or missing data within one working day of these being identified by the CHA operator or within one working day of these being communicated to the CHA by an Emergency Authority (EA). Such discrepancies will be notified to a designated point of contact within the CP.
7. Once a CP has been notified of a discrepancy, the corrected information should be supplied to the CHA within two working days. If there has been no correction from the CP after five working days, the CHA will escalate the issue to its senior contact at the CP.
8. The CHA should keep records of discrepancies in location information supplied by CPs for at least 12 months to assist Ofcom to monitor compliance with GC 4.2.
9. The CP should provide a contact point for the CHA to be able to urgently verify names and addresses against the CP's own records for calls where an EA needs assistance. This contact point should be available 24 hours a day, 365 days a year.
10. If several CPs are involved in calls reaching the CHA, for example where a CP re-sells another CP's services, then all CPs concerned need to co-operate so that appropriate

arrangements for the CLI and associated name and address records to be sent to the CHA are in place and that the above guidelines can be observed.

11. A CP who has exported a number should also transfer the ownership of the associated Emergency Services address record to the importing CP's CUPID. The CP who is now providing service to the end-user should also request to take ownership of the associated Emergency Services address record from the exporting CP's CUPID. These transactions should be placed at the end of the next working day after the number has been successfully exported.

Private Networks of Large Enterprises

- As a minimum, the address provided by CPs to CHAs should be the address of the point of access from private network to the PSTN. (Often the headquarters or largest site for the Enterprise.)
In such cases, the CP should apply an "uncertainty flag" to the address records for the relevant CLIs to alert emergency call handlers to confirm address information verbally with the end user (caller)
- Ensure the Enterprise Customer (Large Corporate customer) understands the limitations for emergency location information from all customer sites.
- CP to advise* the Customer of options** that may allow site-specific location information to be delivered for each access point within its Wide Area Network (WAN) to the 112/999 CHA operators.
- Where a CP has the facility to provide such an option, the CP shall recommend that its customer register and update the location information with it (with accompanying contractual terms). If CPs cannot rely on Enterprise Customer updating the CP, then address records should again be marked with uncertainty flag.

* Where known CP has a reasonable expectation, or has been informed by the Enterprise, that the service is to be accessed from several locations.

** For example, any options recommended by the NICC

<http://www.niccstandards.org.uk/>

APPENDIX 5: MANAGEMENT OF MAJOR INFLUXES OF CALLS - CONFERENCE CALL INVITE AND AGENDA

URGENT OPERATIONAL MESSAGE

999 Service Management Conference Call Invitation/Cancellation

To: Control Room Manager

Details of incident / event (include impact on 999):

The incident/event was detected/estimated to begin at:

Estimated time for restoration of normal service:

Conference call details:

Please join Conference call at _____(time) on _____(date)

Dial in details and pin: 0800 012 1176 pin 41896425#

Required Attendees:

Agenda Chair is BT's 999 Duty manager (normally Glasgow call centre)

1 Introductions

2 999 service situation summary - report from each Control Room along with levels of call delays into the EACR and the CHA

3 Discuss what extra assistance can be offered by neighbouring "buddy" EAs : this needs to include what to do with delayed calls, queue adjustments and announcements, process changes at EAs and whether CHAs including filtering questions. Capture key decisions

4 Need for media announcements, joint statements being used along lines suggested in the PECS Code of Practice. Consider links to other bodies such as Gold or Silver Controls.

5 Recap situation and key decisions.

6 Decide whether or not to reconvene. If so, normally at no less than 30-minute intervals.

Notes: Further background to prepare for Conference Call is to be found in **Section 12** of the PECS Code of Practice

Enquiries or apologies to Telephone Number: 0141 2485813

APPENDIX 6: MOBILE DISCONNECTION

AUTHORITY HEADER & CONTACT DETAILS

MOBILE TELEPHONE DISCONNECTION REQUEST FORM

To: (network) _____

Log Number: _____

Mobile Number _____ has made _____ hoax/malicious emergency calls to _____ (authority name) at the following dates and times.....

We have so far been unable to find the owner of the handset. If we wish to take further action against the owner, we will request any further information through the formal process under IPA.

Description of Call(s):

Please describe in detail what the calls were and, if appropriate, what services were despatched.

Please consider voluntary disconnection of this number for breach of the Communications Act 2003 and your airtime terms and conditions.

This Authority recognises that by disconnecting the mobile number the caller can continue to make calls to the emergency services on a different network (Limited State Service) which means that the phone number will no longer be presented. The impact of this has been taken into account and this Authority accepts the risk on behalf of all emergency services.

We have so far been unable to find the holder of this mobile number. If we wish to obtain further communications data, we will request any further information through the formal process the Investigatory Powers Act 2016.

Requestor's Details

Name: _____ Rank: _____

Signature: _____ Date: _____

Approver's Details

Name: _____ Rank: _____

Signature: _____ Date: _____

APPENDIX 7: IPA REQUEST FOR DATA

REFER TO IPA SPoC FORMS

APPENDIX 8: EMERGENCY CALL MISROUTE AND DETAILS DISCREPANCY

BT 999/112 MISROUTE or PROBLEM REPORT

Completed by:	Email address:
EA Name:	Date:
Tel:	Fax:
This form should be sent by email or faxed to Karen Railton karen.railton@bt.com	

CALL DETAILS

Date of call _____ Time _____ Tel number _____
 Handled by BT Operator Service Centre

Full address of incident including postcode or Easting & Northing

House Number & Street _____
Town / City _____
Postcode _____ **Easting**
/ Northing _____

PROBLEM

A) Call not appropriate to the Fire / Police / Ambulance / Coastguard (**delete as appropriate**)
Action Taken

B) Appropriate but not routed to correct Fire / Police / Ambulance / Coastguard (**delete as appropriate**)
Action Taken

BT RESPONSE SECTION

To: _____ Date _____

BT investigation shows the cause of the problem to be -

Operator error Routing correct according to boundary
 agreement Other

Border routing under investigation Zone Code

Any additional comments

From: Date Tel no

999 CALL NAME & ADDRESS DETAILS DISCREPANCY

CALLING LINE IDENTITY (CLI):		DATE OF 999 CALL:	/ /
EMERGENCY AUTHORITY:		TIME OF 999 CALL:	:

ADDRESS CURRENTLY DISPLAYED AS:

ADDRESS SHOULD BE AMENDED TO SHOW:

Signature:		Tel:	
		Fax:	

**PLEASE E-MAIL PAULA.CRUICKSHANK@BT.COM
OR FAX TO 01332 822285**

***** FOR BT USE ONLY *****

RECEIVED BY:		LOG NUMBER:	/	DATE:	/ /
ACTION TAKEN:					
BT ADDRESS UPDATED	<input type="checkbox"/>	OLO ADDRESS UPDATED	<input type="checkbox"/>	NO AMENDMENT (see comments)	<input type="checkbox"/>
COMMENTS:					
Date Returned to: / / to					

IN CONFIDENCE WHEN COMPLETED

APPENDIX 9: HOAX VOIP CALLS WITH NO ADDRESS DETAILS

There are VoIP CPs that do not allocate individual CLIs to every registered user; this may be because the CP provides some of their customers with an “outgoing calls only” service where it is not possible to call the user back over the CP’s VoIP network.

The CP may therefore use a default or other CLI on emergency calls; for example: - calls originating from the SKYPE network use a default CLI of 05601992020; and calls originating from other CP networks may use the registered user’s mobile phone CLI. The latter may occur where the end user is accessing the VoIP Network via a Wi-Fi app loaded on a mobile device, e.g. Android or i-Phone or even an i-Pad.

SKYPE do offer the following assistance when dealing with hoax calls.

1. To block Hoax caller’s access.

Requests to block hoax caller’s access should be submitted by e-mail to both: - pstn.noc@skype.net and noc@skype.net

Requests should clearly state: -

Request from “X” Emergency Authority to block a 999 Hoax caller. Calls originated at xx:xx hours UK time. (Please list date and times of calls)

2. To request Caller information details.

Note: - SKYPE have advised BT that they will only accept caller information requests from a Police Authority.

Requests should be submitted by e-mail to Skype’s Law Enforcement Compliance department : GLOBALCC@microsoft.com

The request should clearly state: - **Request from “X” Emergency Authority for caller information on a 999 call originated at xx:xx hours UK time.**

APPENDIX 10 EMERGENCY ROAMER ADDITIONAL PROCESS INFORMATION

Please refer to the CSP Crib Sheet for all CP contacts and process detail in relation to the provision of subscriber/location information and arrangements for the disconnection of mobile accounts.

APPENDIX 11: COMMUNICATIONS DATA CODE OF PRACTICE (PURSUANT TO IPA)

Extract from: Investigatory Powers Act 2016 Communications Data Code of Practice

Chapter 10 SPECIAL RULES ON THE GRANTING OF AUTHORISATIONS AND GIVING OF NOTICES IN SPECIFIC MATTERS OF PUBLIC INTEREST

Public Emergency Call Service (999/112 Calls)

10.8 It is usual for telecommunications operators to disclose, at the time of such a call, some identity (caller line identity) and caller location information data (fixed or mobile, if available) to the emergency services in order to facilitate a rapid response to the emergency call.

10.9 Telecommunications operators should take steps to assure themselves of the accuracy of the information they may be called upon to disclose. Any known limitations in this accuracy, particularly for location, should be proactively disclosed to the emergency services. Emergency services should be aware that communications data may not always be available for disclosure by the telecommunications operator depending on the particulars of the communications service used to make the call.

10.10 If the emergency service control room has reason to doubt the address provided for a fixed-line number by the emergency operator (from what the caller has said) then they can contact the Operator Centre in the normal manner and ask for the address to be checked.

10.11 The emergency service can call upon an emergency operator or relevant service provider to disclose data about the maker of an emergency call within the emergency period one hour from the termination of the 999/112 call.

10.12 It is appropriate for the emergency service or emergency operator to require the telecommunications operator to disclose any further caller location information that might indicate the location of the caller at the time of the emergency call. Within one hour of the 999/112 call, it is also appropriate for the telecommunications operator, acting in the belief that information might assist the emergency service to respond effectively or efficiently to the emergency, to proactively disclose to the emergency service or emergency operator any further information about the location of the caller at the time of the emergency call or a new location the caller has moved to, if it is within the one hour period.

10.13 If an emergency call is disconnected prematurely for any reason, technical or otherwise, and the emergency operator is aware or is made aware of this, then the emergency operator can elect to represent the data disclosed when the call was to the emergency service initially. This voluntary disclosure would fall outside the scope of the Act.

10.14 Some telecommunications operators have provided secure auditable communications data acquisition systems for the disclosure of communication data under the Act. Where these exist, it is appropriate for emergency services to be provided with accreditation details to use them for acquiring data about the maker of an emergency call or caller location information, as appropriate, only during the emergency period.

10.15 When a secure auditable system is not available, a manual application for data can be made. The Public Emergency Communications Service Code of Practice contains the process to be followed.

10.16 If the emergency call is clearly a hoax, there is no emergency. Where an emergency service concludes that an emergency call is a hoax and the reason for acquiring data in relation to that call is to detect the crime of making a hoax call – and not to provide an emergency service – then the application process under the Act must be undertaken.

10.17 Should an emergency service require communications data relating to the making of any emergency call after the expiry of the emergency period of one hour from the termination of the call, that data must be acquired or obtained under the provisions of the Act.

10.18 Where communications data about a third party (other than the maker of an emergency call) is required to deal effectively with an emergency call, the emergency service may make an urgent oral application for the data. Disclosure of that data would also fall within under the provisions of the Act.

10.19 Increasingly, members of the public are using non-emergency numbers to request assistance. For instance, a caller might dial either 101 or 111 or other relevant services to seek non-emergency assistance). In some circumstances the call handler may consider it more appropriate that an emergency response is made for instance when the health of the enquirer suddenly deteriorates or a suspect returns unexpectedly to the scene of a crime. In such circumstances the one-hour emergency period and related provisions detailed above apply, even though the number dialled was not an emergency number.

10.20 The Act does not seek to regulate either the actions of the call handler or the provision of data by the telecommunications operator.

ANNEX 12: eSMS MEMORANDUM OF UNDERSTANDING



eSMS MoU May19.docx

ANNEX 13: TELEMATICS PROTOCOL



MOU TELEMATICS Issue
11 (sensitive num