

Lincolnshire Police

Policy Document



Telephone witness statements policy PD 254

Policy document information

Reference number:	PD 254
Policy sponsor:	DCC
Policy owner:	Head of Investigative Standards
Reviewer	DI Tim Woolford
Publication date:	Nov 2024
Review date:	Nov 2026

Version history

Version	Date	Reason for issue
1	Sept 2020	New Policy
2	July 2022	Review of policy - Legislatively and Procedurally compliant as per latest CoP and CPS guidance.
3	Nov 2024	Review

Code of Ethics

All staff involved in carrying out functions under this policy and associated procedures and appendices will do so in accordance with the principles of the Code of Ethics. The aim of the Code of Ethics is to support each member of the policing profession to deliver the highest professional standards in their service to the public.

Legislative compliance

This document has been drafted to comply with the principles of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the staff and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010 and meet our legal obligation in relation to the equality duty. In addition, Data Protection, Freedom of Information and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

Other legislation/law which this policy has been drafted to comply with:

- [Human Rights Act 1998 \(in particular Art 2. Right to Life, Art 8 Right to a Private Life & Art 14 Prohibition of Discrimination\)](#)
- [Equality Act 2010](#)

- [Crime and Disorder Act 1998](#)
- [H&S legislation](#)
- [Data Protection Act 2018](#)
- [Freedom Of Information Act 2000](#)

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes

Authorised Professional Practice (APP)

This policy has been checked against APP and there is none in relation to the subject matter of this policy.

1. Policy aims (Purpose)

- 1.1. Lincolnshire Police has developed a secure method of taking witness statements over the telephone using Pronto on a Samsung or via the Pronto app on a desktop computer. This new process allows more flexibility for the police and witnesses when taking a statement, more efficient working, less travel, and will assist any social distancing measures if required (such as the COVID-19 pandemic). This will also allow a witness statement to be taken from a witness who is outside the country (restrictions in use apply see section 5. The witness could be required to attend court at a later date).

This secure method of taking a telephone witness statement should be used rather than any other process involving the use of email to receive witness statements

- 1.2. This policy and procedure document sets out the scope, procedure and best practice for obtaining a telephone statement with the aim of:

- Ensuring the integrity of a witness's evidence

- Safeguarding witnesses and not compromising safety by taking a statement remotely
- Meeting Information Security requirements
- Streamlining the process of statement taking, when appropriate and safe to do so

2. Policy statement (Key information)

2.1. Background

- 2.1.1. Pronto telephone witness statements functionality allows users to take witness statements over the telephone and send the statement text to a secure web portal for the witness to check and approve. Once approved the statement is finalised and the witness's name and date stamp is added to the statement. The statement is then available on Niche for evidential purposes.

2.2. Implementing the policy

- 2.2.1. This policy relates to the taking of witness statements for criminal proceedings.
- 2.2.2. The functionality is available on Samsung and police laptop computers for police officers, PCSOs, special constables and police staff who take witness statements as part of their role.
- 2.2.2 Procedure – the steps for obtaining a telephone witness statement are as follows: -
- Telephone the witness and confirm their name, date of birth and home address
 - Risk assess the witness to ensure it is safe and appropriate to take a telephone witness statement
 - Create an MG11 through Pronto on a Samsung or a desktop computer

- Select 'telephone statement'. This will auto generate a 6 digit PIN and make the email address box mandatory
- Type the statement while speaking to the witness
- Read the statement back to the witness to confirm the content or make any amendments
- Once the statement content is agreed, select 'complete' and remain on the telephone with the witness
- The statement is sent to the remote portal. This action also generates a unique time restricted (30 minutes) URL and emails it to the witness
- The witness clicks on the URL in the email and is prompted for the six digit PIN and their date of birth
- Read the six digit PIN to the witness over the telephone
- The witness types in the PIN and their date of birth
- The witness is presented with their statement text for review
- The witness reads the statement text and either confirms it by clicking 'approves statement', or clicks 'refuse statement' to reject it
- If **approved**, the statement is finalised and Pronto adds the witness's name and date stamp – this is the electronic signature
- The statement is then available for the officer to view on the relevant Niche Occurrence

If rejected, the officer will have to create a new MG11 and send a new URL to the witness

The officer and witness should remain on the telephone throughout the process of taking the statement.

2.3. Restrictions on the use of telephone witness statements

In all cases the recording officer should assess whether a telephone statement is appropriate, seeking supervisory guidance if required. Key assessment criteria which should be considered as a minimum include: -

- The witness is aged 18 years or over
- A risk assessment has been done and no vulnerability has been identified that could affect the integrity of the evidence at court or the safety of the witness
- The witness agrees to conduct the statement via telephone
- The witness is able to send and receive emails
- The witness does not need an interpreter to speak or read English

2.3.1. There is a need to consider the role of the witness within the investigation.

A professional witness (such as a social worker) may be more suitable for this process than a victim of crime.

In all cases, an investigator must take into account all of the factors that are referred to in the policy (e.g age, vulnerability etc) – including the crime type – and then having considered all of these (including their connection to the crime) make a determination on the best way to obtain the evidence. If there is then a suitable rationale for obtaining the evidence by way of telephone – even in a major or serious investigation then this can be completed.

Particular care should be taken to consider the suitability or otherwise of this sort of process if:

- The crime involved
 - Honour based abuse
 - Forced Marriage
 - FGM
 - High risk Domestic Abuse (DA)
 - Sexual Exploitation
 - Serious Hate Crime
- Where there is evidence of Criminal Exploitation and/or Modern Slavery

- The offence is a RASSO (Rape and Serious Sexual Offence), including sexual offences involving multiple victims; vulnerable adults; youth victims or defendants; voyeurism
- The witness is vulnerable e.g. elderly, significant diagnosed Mental Health issues or learning disabilities, or the witness meets the NPCC definition of vulnerability – ‘a person is vulnerable if as a result of their situation or circumstances, they are unable to take care of, or protect themselves, or others, from harm or exploitation.’
- The witness needs an Appropriate Adult
- It is not possible to establish Mental Capacity
- The witness requires an interpreter
- It is a First Statement and there is significant DA history

It may be appropriate to take a telephone witness statement for a DA incident if:

- The DA is graded as standard risk and a face-to-face DASH has already been completed with the victim AND
- A face-to-face initial witness statement and DASH have already been obtained and an additional supplementary statement is required from the victim and there is no element of coercive control

Particular care should be taken when a telephone statement is taken from a VICTIM of crime within these areas. What may be appropriate in terms of seeking evidence from a witness may not be appropriate when obtaining an account from a victim in view of the potential vulnerability and ongoing concerns exhibited as a result of these sorts of crime. It is imperative that appropriate support be offered and therefore any decision to use telephone statements from victims in these circumstances should always be discussed with a supervisory officer.

2.4. Public facing web portal

The public web portal will be a new component built specifically for this purpose. It will be an internet-facing service shared by all Pronto customers

who use the remote statements functionality. It will be hosted on an Azure instance within the UK.

The public portal will have two entry points:

- An API that Pronto hubs will use to send and receive data from
- A front end allowing witnesses to visit the URLs they've been emailed and confirm statement wording.

2.4.1. Public Portal Security

The Remote statements public portal consists of two components, a service and a web user interface.

The Remote statements service is a microservice, running in Azure, providing a REST API, accessed over HTTPS.

The Remote statements web UI is an Angular web application, running in Azure, accessed over HTTPS. The web UI calls REST endpoints on the microservice to access and update data.

2.4.2. Uploading a statement

To communicate with the service, firstly, Pronto Hub must make a service to service authentication request to a Motorola managed Identity management system running in Azure using Open ID Connect and the OAuth Client Credentials Flow. This provides Pronto Hub with an OAuth access token that can be used to communicate with the service. The client credentials individually identify the customer. Access tokens have an expiry time of 2 hours (requiring regular re-authentication by Pronto Hub).

Pronto Hub then uploads a statement by calling a REST API using HTTPS. The HTTPS request uses TLS 1.2, and TLS is managed by a FIPS-140-2 approved gateway in Azure. The Remote statements service validates the OAuth token (against the identity management system) to check that it is a valid token, has not expired, and has not been revoked, and that it is valid for the particular customer.

The Remote statements service stores the statement temporarily in an Azure Cosmos database. The database is firewalled off to prevent access from anything other than the Remote witness service. In addition, the database is protected by an Azure SAS token (a secure token, required to access the service, stored in a secure Azure keyvault, and accessible only to the Remote statements service). The statement is stored with a time to live. It will be automatically deleted after this period to prevent data leakage. This time to live value will be provided by Pronto Hub (when the statement is uploaded) and can be managed by customer site configuration.

All data stored in Azure Cosmos is encrypted at REST with FIPS-140-2 approved AES-256 encryption. <https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-fips-140-2?view=o365-worldwide>

The Remote statements service will return a URL to Pronto. This URL is sent by email (by Pronto) to the witness.

Requests to upload statements will be audit logged in the cloud. Audit logs contain customer name, statement id, date/time but do not contain personally identifiable information.

2.4.3. Retrieving a response

Pronto Hub will retrieve data from Remote statements service from an Azure Service Bus.

Pronto Hub uses the access token retrieved from the identity management system to call an HTTPS REST endpoint on the Remote statements service to retrieve a Shared Access Signature (SAS) token. The Remote statements service validates the access token (as above), validates the customer, and enables a topic and subscription for the particular customer. The Remote statements service manages and sends data to the service bus using a SAS token held securely in Azure Key Vault, and only accessible to the Remote Statements service. The remote statements service generates a temporary SAS token that can be used to connect to the specific customer topic, and is valid for a period of 2 hours.

Pronto Hub uses this token to connect to the Azure service bus topic subscription (using AMQP messaging protocol, over TLS 1.2). The Azure service bus validates the token, before permitting Pronto Hub to connect. Pronto Hub is then able to retrieve responses from Remote statements service. Pronto Hub only needs to make an outgoing connection to the service bus removing any need for incoming network connections into the Force network.

2.4.4. Two Factor Authentication

The user requires to have access to a valid, cryptographically signed, time limited URL, and requires to know their own date of birth and the six digit security code (unique to the statement). In addition, the Remote statements service will keep track of failed attempts to enter a date of birth & security code (with a valid statement link). If this exceeds a configurable maximum number (five?) then the statement will be automatically deleted and Pronto will be notified. This prevents any brute force attempt to access the statement should some gain access to the witness's email account and gain access to the signed URL.

3. Other related documents and appendices

3.1. Related documents:

- Safeguarding Children Policy - PD 113
- Attendance Policy

Other Considerations:

- Modern Slavery
- Adult Safeguarding and Protecting most Vulnerable

4. Monitoring and review

- 4.1 The policy will be subject to periodic review by the Head of the FCR on a biennial basis to maintain compliance with legislative updates and to reflect good practice adopted from other Forces.

5. Who to contact about this policy

- 5.1. Any enquires about this policy should be directed to the Crime Standards Team at HQ.