- any compromise or suspected compromise of COMINT material must be reported immediately to the COMSO and a security incident report sent to Security as soon as practicable after the incident or suspicion
- all records are available for audit by the COMSO at any time.

AFP appointees who supervise or otherwise work with other AFP personnel who handle COMINT material must ensure that those AFP personnel comply with the COMINT material requirements as detailed above.

Any compromise or suspected compromise of COMINT material must be reported by the COMSO to the Department of Defence.

26.5 Transmission of classified material

Codeword material and information classified TOP SECRET must:

- never be stored or transmitted on standalone computers or networks other than the AFP Top Secret Network (AFPTSN)
- be stored within a SCIF in accordance with the access and storage requirements for information and assets
- not be removed from a SCIF or AFP premises unless:
    - the material is stored in a Security Construction and Equipment Committee endorsed container in accordance with the access and storage requirements for information and assets
    - written approval for the movement is received from the originating author, agency or business unit
    - the Top Secret Control Officer has approved the movement
    - movement is recorded in the relevant CDR
    - the classified information is managed in accordance with the AFP Information handling guides, and safely transfer in accordance with Attachment 2 of this guideline.

26.6 Waste management

Regardless of its protective marking, any document no longer required within a Zone 5 area or SCIF must be shredded using an approved Class A shredder. The destruction must be:

- conducted by two AFP appointees who hold the necessary security clearance and briefings
- notated in the relevant CDR as destroyed (the destruction member and witness must sign the register)
- in accordance with this guideline and the AFP National Guideline on information management.

All printer cartridges must be sanitised prior to removing them from the machine in accordance with the procedures detailed in the information handling guides and the Australian Government Information Security Manual. Sanitised cartridges must be provided to the COMSO for destruction.

General waste must be kept in bins separate to those used for classified documents.

27. Communications security risk management

27.1 Phone and multifunction devices

The AFP deploys a suite of secure phone, fax and multifunction devices inside Zone 4, Zone 5 and locally designated sensitive areas. These communication systems provide secure communications within the AFP and with external agencies.

When communicating classified material via telephone, AFP appointees must use the appropriate phone systems as listed in the table below:

Phone system	Classification
Avaya VoIP phones	UNCLASSIFIED
AFPSec VoIP	up to and including SECRET

AFPTSN VoIP	up to and including TOP SECRET

AFP appointees who supervise or otherwise work with other AFP personnel must ensure those AFP personnel use the appropriate phone systems as listed in the table above when communicating classified material.

Handsets with 'push to talk' switches installed must not be modified or otherwise tampered with which would render the capability ineffective.

In all areas where SECRET ICT systems are located and fitted with VoIP phones, mobile phones and other VoIP systems of lower classifications may be used if appropriate standard operating procedures to prevent data spills exist and are adhered to.

27.2 Infrared data association communication devices

All infrared data association devices, such as remote control handsets, which form part of the operational fixtures of a Zone 5 area or SCIF, must only be installed after both:

- certification by technical surveillance counter measures
- receipt of a written security waiver from the Manager Security (Chief Security Officer).

27.3 Controlled cryptographic (encryption) items

All controlled cryptographic items are the responsibility of the Security portfolio and must only be purchased and maintained by Security in accordance with Australian Signals Directorate (ASD) guidelines.

To protect against interception and/or unauthorised reading of misrouted data, system users must only use ASD approved encryption devices when using AFP voice and data communication devices to transmit information classified CONFIDENTIAL or above.

For information on ASD approved devices contact Security.

27.4 Cryptographic systems/equipment

Cryptographic (encryption) software or devices must not be installed on, or connected to, AFP ICT systems unless the installation is approved and coordinated by Security.

Unless specifically authorised by Security, system users must not install encryption software products (freeware, shareware or commercial) on any AFP ICT system.

Encryption devices and cryptographic key material must be managed by Security in accordance with Australian Communications-Electronic Security Instructions.

System users must afford cryptographic key material and associated equipment the level of physical protection commensurate with its security classification in accordance with instructions from Security.

Should an encryption device fail, where a backup link does not exist, system users must suspend the communication link pending the installation of a replacement device, unless otherwise authorised by the system risk owner after consultation with Security.

28. Security incidents

Any breaches of this guideline must be reported to AFP Security via a security incident report form.

In addition to breaching the professional standards of the AFP, inappropriate departures from the provisions of this instrument may also constitute a breach of AFP's security and be dealt with under the security incident management practices, as per the AFP Commissioner's Order on Security (CO9).

To enable the Manager Security (Chief Security Officer) to notify system risk owners of any data spill, security incidents involving AFP and third party ICT systems must be notified in accordance with security reporting requirements, refer to Part C of the AFP National Guideline on personnel security. Failure to comply with system security requirements may result in either the temporary suspension or permanent withdrawal of services by the system risk owner.

Note: the cost of data spills may be passed back to the business unit responsible. To limit the cost incurred to the business area the incident must be reported to Security as soon as practicable after the incident occurs.

29. Further advice

Queries about the content of this document should be referred to Security Reporting & Referrals.

30. Resources

Legislation

- *Archives Act 1983* (Cth)
- *Australian Federal Police Act 1979* (Cth)
- *Privacy Act 1988* (Cth) (including the Australian Privacy Principles).

AFP governance instruments

- AFP Commissioner's Order on Professional Standards (CO2)
- AFP Commissioner's Order on Security (CO9)
- AFP National Guideline for official online activities
- AFP National Guideline on access to PROMIS by non-AFP appointees
- AFP National Guideline on Complaint Management
- AFP National Guideline on information management
- AFP National Guideline on intellectual property, commercialisation, logos and insignia
- AFP National Guideline on integrity reporting
- AFP National Guideline on mobile devices
- AFP National Guideline on personnel security
- AFP National Guideline on physical security
- AFP National Guideline on procurement and contracting
- AFP National Guideline on social media (drafting)
- Better Practice Guide on applying protective marking
- Better Practice Guide on Workplace Bullying and Workplace Discrimination.

Other sources

- Access and storage requirements for information and assets
- AFP asset management guidance
- AFP Corporate Forms and Templates
- AFP Discussion Fora
- AFP Information handling guides
- AFP Security Governance Framework
- AFP Security Glossary of Terms
- AFP System risk owners
- Australian Communications-Electronic Security Instructions (Security)
- Australian Government Business Impact Levels
- Australian Government Cabinet Guideline
- Australian Government Cloud Computing Policy
- Australian Government Information Security Manual
- Australian Government Protective Security Policy Framework
- How to Sanitise AFPNet Printer
- Information handling guides
- International Travel Approval Form
- Internet Browsing Categories, allowed and blocked

- Mobile electronic devices returning from travel FAQs
- Protective Security Policy Framework (PSPF): Security zones and risk mitigation control measures
- PSPF – Australian Government Physical Security Management Protocol
- Removable data storage devices FAQ
- Security classifications of email allowed to organisations
- Security ICT system audit plan (Information Security)
- Security incident report
- Travelling internationally with electronic devices guide
- Documentation which can be obtained from the Communications Intelligence Security Officer:
    - s7(2)
    - s7(2) Technical Note
    - Protective Security Circulars
    - s7(2) – can be obtained from the s47E(d)
    - Department of Foreign Affairs and Trade Special Security Orders and Standing Instructions.

31. Attachments

Attachment 1 – Prohibited items

The items listed in the table below are prohibited from:

- audio secure rooms
- locally designated sensitive areas
- Sensitive Compartmented Information Facilities (SCIF)
- speech privacy rooms
- Zone 5 areas.

ITEM	DESCRIPTION
1	Mobile device
2	iPad/iPod
3	Device with Bluetooth or GPS connectivity
4	Camera or Film
5	Memory stick or card
6	Recording device
7	Activity fitness tracker
8	Smart watch
9	Bag, Briefcase or Document Holder

Attachment 2 – Transferring and transporting classified information

Attachment 2 – Transferring and transporting classified information

Attachment 3 – Classified documents accountability

1. Classified Document Register entries

Where multiple copies of the same document are received or made, each individual copy of the document requires registration as a separate entry in a Classified Document Register (CDR).

All CDR working entries must be made in black or blue (non-erasable) ink with the exception of:

- temporary disposal entries, which may be made in pencil
- deletions, which must be made in red (non-erasable) ink
- entry dates as detailed below.

Entries may be abbreviated to enable more detailed information to be recorded.

Date of entries

For each new day, the date the entries are made in the CDR must be written in red on the next available blank line which is not serial numbered.

Documents must be entered in the CDR as soon as they have been received or printed and prior to their distribution or removal from AFP facilities.

Covering letters

Where a document is accompanied by a covering letter of a classification not requiring registration, care should be taken to ensure the parent document is marked as being registered; not the covering letter.

Where more than one document of a classification requiring registration is sent under the same covering letter, each separate document must be registered.

Receipt details

RECEIPT OR ORIGIN DETAIL							
Serial No. (a)	Type of Document (b)	Sender or Originator (c)	Reference Number (d)	Date of Origin (e)	Title (or Subject) (f)	Classification (g)	Copy Number (h)

Table 1 - CDR receipt page

The CDR receipt page reproduced at Table 1 must be completed as follows:

- Allocated serial numbers in column (a) must be marked on the respective document as part of the registration process. Serial numbers must be sequential from the first CDR entry on the first page to the last CDR entry on the last page.
- Document types in (b) should stipulate whether it is a letter, intelligence report, photograph, compact disc, etc.
- Entries in columns (a) to (i) (refer to Tables 1 above and 2 below) must be completed immediately after documents are received or printed from an ICT system.
- Every copy of each document must be recorded as separate entries so that subsequent disposal can be clearly tracked.
- in column (g) abbreviations for protective markings are sufficient.
- where documents are copy numbered (h), the number must be recorded as ‘copy # of #’; otherwise place a hyphen in this column.

When classified documents are received in envelopes marked ‘Personal for…’, ‘Exclusive for…’ or as ‘Eyes only’ for a person or nominated position, the CDR maintaining member (CDRMM) must deliver by hand or safehand the unopened envelope to the intended recipient. On delivery, the addressee must be asked to:

- inspect the package to ensure it has not been tampered with or otherwise compromised
- open the item and ensure the CDRMM is appropriately cleared and briefed to handle the document
- pass the contents to the CDRMM (if appropriately cleared) or to another appropriately cleared person for registration and filing.

Once registered and filed, the documents must be referred back to the intended recipient for any other action required.

Disposal details

DISPOSAL DETAILS					
	TEMPORARY		FINAL		REMARKS
Total Number Received or Produced (i)	Referred to and Date (j)	Returned and Date (k)	Despatched to or Enclosed in (Ref No of File and Folio No) (l)	Receipt Serial No and Date Returned (m)	(Include destruction particulars when applicable or signature of recipient where receipt is not used) (n)

Table 2 - CDR disposal page

The CDR disposal page reproduced at Table 2 must be completed as follows:

- where more than one copy of a document is either produced or received, indicate in column (i) how many (e.g. where 3 copies of a document are received or produced, the number '3' must be placed in column (i) for each of the 3 required entries)
- the CDRMM must check columns (j) and (k) to ensure that documents are not on temporary disposal for more than 48 hours and that when complete, the entry is closed and final disposal completed
- final disposal for all entries to a file (show folio number) is shown in column (l)
- final disposal for all entries to an addressee is shown in column (m)
- entries for documents that have been retained locally remain open and are accountable until they are closed by destruction or further disposal of the related document or material
- entries relating to the receipt of amendments should be endorsed in column (n) as 'incorporated into CDR serial.....', then deleted by red entry
- column (m) must be completed immediately after the receipt form is returned for incoming items or raised for outgoing items
- column (n) must contain all detail of a document's destruction, including the full details of any witnesses to the destruction. Other comments applicable to the chain of custody of the document should also be entered
- where a recipient signs for a document in the CDR, their AFP number (or other relevant identification number), name, date and signature must be recorded in column (n).

Safe-hand receipt forms

All CDR-related receipt forms must be returned:

- within Australia: within 14 days of the date of receipt
- overseas: within 30 days of the date of receipt.

CDRMMs must actively monitor the return of receipts. Where documents have not been received by the intended recipient, the sender must commence tracing the path of the documents to identify their current location.

If tracing action fails to locate the documents, Security-Reporting-and-Referrals must be notified via a security incident report as per the AFP National Guideline on personnel security.

Destroying registered documents

When classified documents require destruction, the following procedure must be applied:

1. The destruction must be conducted by a CDRMM.

2. Prior to any destruction occurring, each document to be shredded must be positively identified by both the CDRMM and a witness, by cross-checking the details on the document with the details recorded in columns (a) to (h) of the CDR.
3. TOP SECRET documents must be shredded within the relevant sensitive compartmented information facility (SCIF).
4. All parts of each document must be destroyed using a Class A shredder.
5. Once the documents have been destroyed, the CDRMM must close the relevant CDR entries by conducting the actions detailed below.

When non-paper documents (i.e. CDs, DVDs, etc.) require destruction, the Communications Intelligence Security Officer (COMSO) must be consulted to determine the appropriate method of destruction.

Shredding particles must be collected in a clear plastic bag attached to the shredder. Once an appropriate AFP appointee of the area (i.e. who has the necessary security clearance and briefings) has checked that all of the shredding is 1mm cross-cut, it may be disposed of as UNCLASSIFIED waste. To make it easier to check for large pieces, other forms of paper waste or non-paper waste must not be mixed with the shredded material.

Closing a CDR entry

When there is no longer a need to retain a document within the originating business area, it can be:

- disseminated in accordance with Commonwealth law and the AFP National Guideline on information management
- archived if required per the *Archives Act 1983* (Cth) and the AFP National Guideline on information management
- destroyed by shredding in a Class A shredder.

In each case, the applicable CDR entry must be closed by ruling a red line straight across both the Receipt Details page and Disposal Details page along the middle broken line. Where a document is disposed of by transfer to another person using a safe-hand receipt, the entry may only be closed on return of the receipt form.

Where a document has been shredded, the destroying CDRMM and witness must clearly write their names and AFP numbers, and date and sign the entry in column (n).

Archiving registered documents

TOP SECRET documents must not be submitted to the AFP's Records Management Unit.

Registered documents that need to be archived should be delivered by safe-hand, as per Attachment 2 of this guideline, to the nearest regional AFP Records Management office. The AFP's Records Management office responsible for archiving must sign for each document, and **note** the file in which the documents are contained.

Audits

If an item recorded in a CDR cannot be located during an audit, the Security Reporting requirements must be followed.

The details/results of audits/musters must be recorded separately to the material held against the CDR and vice versa. The record must include the:

- date of the audit
- serial numbers checked
- method used for the audit (e.g. all documents in a file (insert file numbers), sequential CDR serial numbers, etc.)
- anomalies identified and corrective action taken.

2. Closing and retention of CDRs

A CDR remains active until all entries have been closed. Once all entries awaiting destruction, disposal or transfer to another CDR have been completed, the CDR may be closed.

The CDR must be retained by the business area for 5 years after the date it was closed.

In the event that a team or function is disbanded or re-organised, the return and transfer of all accountable material held by that team or portfolio is the responsibility of both the outgoing CDRMM and responsible line manager. Once all accountable material has been returned or disposed of, the CDR must be returned to the Information Security-Communications Security Team/COMSO.

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 11:42 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47B invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 11:18 PM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 2 December 2019 2:46 PM
To: s47E(d)
Subject: Verify your email for Clearview

Hi s47E(d)

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/ImNyYWlnLm1hbm5AYWZwLmdvdi5hdSI.EMYogA.sR0hWHJs3lwNLOB39UhXXm-cjW0

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 2 December 2019 2:46 PM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

s47E(d)

From: Hoan T s47G @clearview.ai>
Sent: Tuesday, 3 December 2019 2:13 PM
To: s47E(d)
Subject: Connecting re: Clearview

Hi s47E(d)

I'm one of the founders of Clearview - and also incidentally from Australia, but now living in the USA

How have you found the app so far? I would love to connect and learn more about how it can be used for the AFP.

Let me know what time is good to chat!

Best Regards
Han

s47E(d)

s47E(d)

From: s47G @clearview.ai>
Sent: Tuesday, 3 December 2019 2:46 PM
To: s47E(d)
Subject: Re: Connecting re: Clearview [SEC=UNOFFICIAL]

Great chatting s47E(d)

Just let me know the names/emails of any colleague you want to give the app too

Let's stay in touch!

> On Dec 2, 2019, at 11:18 PM, s47E(d) @afp.gov.au> wrote:
>
> UNOFFICIAL
> Hi Han,
>
> Thanks for reaching out. We've only just started using it and so far it has been valuable.
>
> I'm available anytime.
>
> Rgds
>
> s47E(d)
>
> COVERT ONLINE ENGAGEMENT
> AUSTRALIAN CENTRE TO COUNTER CHILD EXPLOITATION AUSTRALIAN FEDERAL
> POLICE
>
> Tel + s47E(d) www.afp.gov.au
> UNOFFICIAL
>
> -----Original Message-----
> From: Hoan T s47G @clearview.ai>
> Sent: Tuesday, 3 December 2019 2:13 PM
> To s47E(d) @afp.gov.au>
> Subject: Connecting re: Clearview
>
> Hi s47E(d)
>
> I'm one of the founders of Clearview - and also incidentally from
> Australia, but now living in the USA
>
> How have you found the app so far? I would love to connect and learn more about how it can be used for the AFP.
>
> Let me know what time is good to chat!
>
> Best Regards
> Han
>
> **********
> WARNING

>
> This email message and any attached files may contain information that
> is confidential and subject of legal privilege intended only for
> use by the individual or entity to whom they are addressed. If you
> are not the intended recipient or the person responsible for
> delivering the message to the intended recipient be advised that you
> have received this message in error and that any use, copying,
> circulation, forwarding, printing or publication of this message or
> attached files is strictly forbidden, as is the disclosure of the
> information contained therein. If you have received this message in
> error, please notify the sender immediately and delete it from your
> inbox.
>
> AFP Web site: http://www.afp.gov.au
> **********

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 5 December 2019 12:27 AM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:55 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Tuesday, 17 December 2019 1:13 AM
To: s47E(d)
Subject: Your Clearview account is still waiting

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 9 January 2020 6:40 PM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:52 AM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.