

Shared Banned List Protocols – Server End

- ID-Tect operates a secured server that only allows access to a designated TCP port allowed thro the firewall. All Server calls are validated thro a unique registration code assigned to each participating idEye user.
- All ID images uploaded/downloaded is encrypted and water marked
- Only banned data is uploaded to ID-Tect server.
- The contents of the ban list are strictly confidential.
- Record all deletions in the deletion book.
- Shared Banned list data is only aaccessed by appointed data entry person, Technical Support Manager and the Managing Director.
- Identify individuals requesting details of their ban via telephone by their name and D.O.B
- Check notes for spelling mistakes and crude or libellous statements.
- Re-word if the context can be maintained or delete it.
- Delete bans which contain a blank note page.
- Contact establishment if notes are sparse or vague for more detail, delete if not provided.
- Delete expired bans.

Venue Protocols

- That management and staff will take all reasonable measures to protect the privacy of individuals whose details have been stored and/or retrieved by idEye whether as a patron or as a banned person
- To change the passwords periodically (immediately upon knowledge of a compromised password)
- That the venue must provide a secured and reliable network connection
- The privacy statement must be displayed at all times when idEye is in use

What the participating Venues can do to keep the information safe?

- Only grant basic access to the operator – controlled access
- Change administrative password regularly or if compromised
- Engaged ID Guard to block address and ID image
- Make sure that your Local Area connection is secured thro your local IT service provider
- Your data is stored on your local idEye unit, only banned list is shared. Don't leave your hardware unattended and logged in. Log-off if unattended or left idle for a longer period of time.

FAQ's

How long are records kept?

It is recommended that all records of entry are retained for up to 28 days in line with CCTV recordings. This allows a reasonable time period for any complaints or incidents to surface.

Who is able to access the data recorded?

Data is password protect and can only be accessed by authorised managers.

Is the person recording the identification able to view an individual's details?

The doorman can only view the current entry on the screen whilst it is being scanned.
(if Restrict Patron Navigation function is engaged)

How long does a ban remain effective?

A ban remains in effect until the ban period expires and is removed by an authorised person.

What banned list information is shared amongst the participating venues?

Patron file photo, Name, DOB and ID Number for verification.

Who else has access to my scanned data apart from the shared ban list?

No one else apart from your authorised management has any access to scanned your records.

What if someone within my staff copies a scanned ID on to a USB drive?

All scanned copies of ID's are encrypted and watermarked thus cannot be opened with any other program other than idEye