Expose360 Database Tables Structure

Table 1: users

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique user identifier
name	VARCHAR(100)	NOT NULL	User's full name
email	VARCHAR(100)	UNIQUE, NOT NULL	User's email address
phone	VARCHAR(20)	UNIQUE	User's phone number
password_hash	VARCHAR(255)	NOT NULL	Encrypted password
status	ENUM('active', 'inactive')	DEFAULT 'active'	Account status
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Registration date
updated_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP ON UPDATE	Last modification date

Table 2: admins

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique admin identifier
name	VARCHAR(100)	NOT NULL	Admin's full name
email	VARCHAR(100)	UNIQUE, NOT NULL	Admin's email address
phone	VARCHAR(20)	UNIQUE	Admin's phone number
password_hash	VARCHAR(255)	NOT NULL	Encrypted password

Column Name	Data Type	Constraints	Description
is_master	BOOLEAN	DEFAULT FALSE	Master admin flag
status	ENUM('active', 'inactive')	DEFAULT 'active'	Account status
created_by	INT	FOREIGN KEY → admins(id)	Admin who created this account
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Account creation date

Table 3: employees

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique employee identifier
name	VARCHAR(100)	NOT NULL	Employee's full name
email	VARCHAR(100)	UNIQUE, NOT NULL	Employee's email address
phone	VARCHAR(20)	UNIQUE	Employee's phone number
status	ENUM('active', 'inactive')	DEFAULT 'active'	Employment status
assigned_by	INT	FOREIGN KEY → admins(id), NOT NULL	Admin who assigned employee
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Assignment date

Table 4: posts

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique post identifier

Column Name	Data Type	Constraints	Description
user_id	INT	FOREIGN KEY → users(id), NOT NULL	Post author
title	VARCHAR(255)	NOT NULL	Post title
description	TEXT	NOT NULL	Post content/details
category	ENUM('crime', 'corruption', 'public_safety')	NOT NULL	Post category
verification_status	ENUM('pending', 'verified', 'rejected')	DEFAULT 'pending'	Verification state
is_published	BOOLEAN	DEFAULT FALSE	Publication status
is_deleted	BOOLEAN	DEFAULT FALSE	Soft delete flag
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Post creation date
updated_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP ON UPDATE	Last edit date

Table 5: post_media

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique media identifier
post_id	INT	FOREIGN KEY → posts(id), NOT NULL	Associated post
media_type	ENUM('photo', 'video', 'live')	NOT NULL	Type of media
file_path	VARCHAR(500)	NOT NULL	Storage path
verification_status	ENUM('pending', 'verified', 'rejected')	DEFAULT 'pending'	Verification state
ai_check_result	ENUM('real', 'ai_generated', 'uncertain')	DEFAULT 'uncertain'	AI verification result

Column Name	Data Type	Constraints	Description
is_duplicate	BOOLEAN	DEFAULT FALSE	Duplicate detection flag
uploaded_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Upload timestamp

Table 6: verification_logs

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique log identifier
media_id	INT	FOREIGN KEY → post_media(id), NOT NULL	Media being verified
verified_by	VARCHAR(100)	-	Verifier (employee/AI)
verification_method	ENUM('ai_api', 'ml_model', 'manual', 'duplicate_check')	NOT NULL	Method used
result	ENUM('passed', 'failed')	NOT NULL	Verification result
notes	TEXT	-	Additional comments
verified_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Verification timestamp

Table 7: toon_tokens

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique token identifier
token_id	VARCHAR(255)	UNIQUE, NOT NULL	TOON hash value
post_id	INT	FOREIGN KEY → posts(id), NOT NULL	Associated post

Column Name	Data Type	Constraints	Description
user_id	INT	FOREIGN KEY → users(id), NOT NULL	Token owner
content_hash	VARCHAR(255)	NOT NULL	Content integrity hash
is_immutable	BOOLEAN	DEFAULT TRUE	Cannot be changed flag
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Token generation time

Table 8: otp_requests

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique OTP identifier
email	VARCHAR(100)	NOT NULL	Requester's email
otp_code	VARCHAR(6)	NOT NULL	6-digit OTP code
expires_at	DATETIME	NOT NULL	Expiration time (1-2 min)
is_used	BOOLEAN	DEFAULT FALSE	Usage status
created_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Request timestamp

Table 9: deleted_users

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Deleted record identifier
original_id	INT	NOT NULL	Original user ID
name	VARCHAR(100)	NOT NULL	User's full name
email	VARCHAR(100)	NOT NULL	User's email address
phone	VARCHAR(20)	-	User's phone number
password_hash	VARCHAR(255)	NOT NULL	Encrypted password

Column Name	Data Type	Constraints	Description
status	VARCHAR(20)	-	Last known status
deleted_by	INT	NOT NULL	Admin who deleted
deleted_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Deletion timestamp
can_restore	BOOLEAN	DEFAULT TRUE	Restoration permission
original_created_at	TIMESTAMP	-	Original creation date

Table 10: deleted_admins

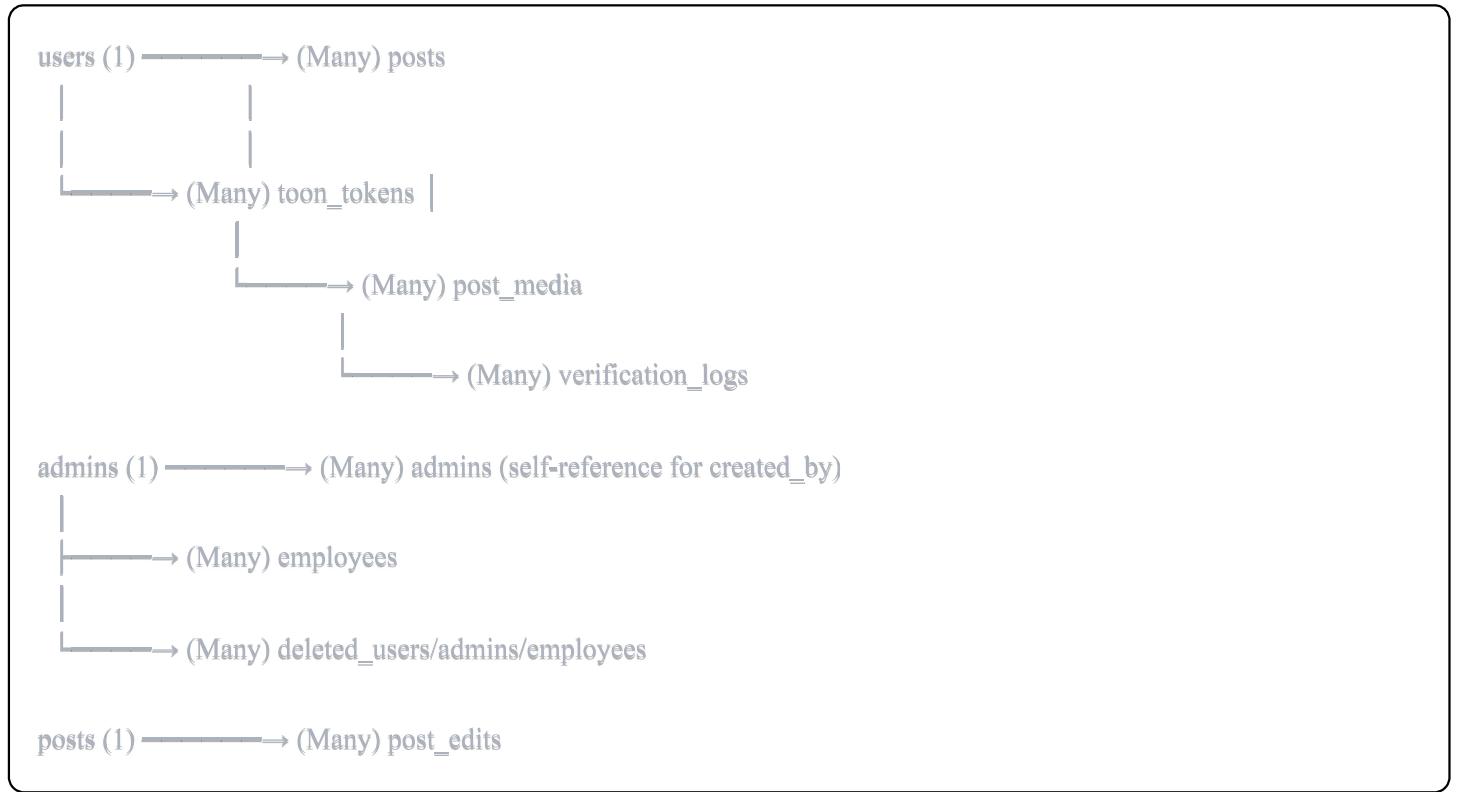| Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Deleted record identifier
original_id	INT	NOT NULL	Original admin ID
name	VARCHAR(100)	NOT NULL	Admin's full name
email	VARCHAR(100)	NOT NULL	Admin's email address
phone	VARCHAR(20)	-	Admin's phone number
password_hash	VARCHAR(255)	NOT NULL	Encrypted password
is_master	BOOLEAN	-	Master admin flag
status	VARCHAR(20)	-	Last known status
created_by	INT	-	Who created this admin
deleted_by	INT	NOT NULL	Admin who deleted
deleted_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Deletion timestamp
can_restore	BOOLEAN	DEFAULT TRUE	Restoration permission
original_created_at	TIMESTAMP	-	Original creation date

Table 11: deleted_employees

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Deleted record identifier
original_id	INT	NOT NULL	Original employee ID
name	VARCHAR(100)	NOT NULL	Employee's full name
email	VARCHAR(100)	NOT NULL	Employee's email address
phone	VARCHAR(20)	-	Employee's phone number
status	VARCHAR(20)	-	Last known status
assigned_by	INT	-	Admin who assigned
deleted_by	INT	NOT NULL	Admin who deleted
deleted_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Deletion timestamp
can_restore	BOOLEAN	DEFAULT TRUE	Restoration permission
original_created_at	TIMESTAMP	-	Original assignment date

Table 12: post_edits

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO_INCREMENT	Unique edit identifier
post_id	INT	FOREIGN KEY → posts(id), NOT NULL	Edited post
user_id	INT	FOREIGN KEY → users(id), NOT NULL	User who edited
field_changed	VARCHAR(50)	NOT NULL	Which field was edited
old_value	TEXT	-	Previous value
new_value	TEXT	-	New value
edited_at	TIMESTAMP	DEFAULT CURRENT_TIMESTAMP	Edit timestamp

Database Relationships Diagram

```
users (1) ─────────→ (Many) posts
  │                      │
  │                      │
  │                      │
  └──────→ (Many) toon_tokens │
                  │
                  └──────→ (Many) post_media
                              │
                              └──────→ (Many) verification_logs

admins (1) ─────────→ (Many) admins (self-reference for created_by)
  │
  ├──────→ (Many) employees
  │
  └──────→ (Many) deleted_users/admins/employees

posts (1) ─────────→ (Many) post_edits
```

Key Features Summary

✅ **Separate User & Admin Tables**

- Different authentication flows
- Different permission levels
- Better security management

✅ **Active/Inactive Status**

- Both users and admins have status field
- Can disable accounts without deleting

✅ **Soft Delete System**

- Deleted records moved to separate tables
- Can be restored by admins

- Maintains data integrity

✅ **Master Admin Protection**

- `is_master` flag in admins table
- Cannot be deleted (business logic)
- Always has full privileges

✅ **Content Verification**

- Multi-step verification process
- AI and manual verification logs
- Duplicate detection

✅ **TOON Token System**

- Immutable content proof
- Hash-based integrity
- Timestamp verification

✅ **Security Features**

- Password hashing (BCrypt)
- Time-based OTP (1-2 minutes)
- Edit history tracking