Software Requirements Specification

for

Smart Parental Controls

Version 1.0 approved

Prepared by

S.D.D.N.Sudasingha

s23010374

625399072

06.06.2025

Project: Smart Parental Controls — Smart Parenting and Family Management App

Domain: Parenting and Family

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Team Alpha	2025-06-01	Initial draft creation for Parental Control & Monitoring App	1.0

1.Introduction

Parental controls are tools and features built into digital television services, computers, video games, mobile devices, and software that help parents manage what their children can access and do. These controls let parents block or limit content they believe is inappropriate for their child's age, maturity level, or simply better suited for adults.

1.1 Purpose

This document defines the software requirements for a Parental Control System. Parental controls are features included in digital televisions, computers, video games, mobile devices, and software that allow parents to restrict access to content they feel is inappropriate for their child's age, maturity level, or developmental stage.
The SRS will outline how the system will provide these controls, ensuring parents can manage, monitor, and guide their children's digital use.

1.2 Document Conventions

This document adopts the following conventions to ensure clarity and consistency:

- Clear, hierarchical headings to organize content.
- Requirements are written in simple, direct, and actionable language.
- Features and controls are categorized based on established parental control domains:
    - Content Filters: Limit access to age-inappropriate material.
    - Usage Controls: Restrict time spent or types of usage on devices or apps.
    - Computer Usage Tools: Allow or restrict access to specific software or applications.
    - Monitoring: Track user activity or location when permitted.

These conventions help all readers—technical or non-technical—understand the scope, purpose, and expectations of the system.

1.3 Intended Audience and Reading Suggestions

This Software Requirements Specification (SRS) is intended for the following groups:

- Developers: To understand the system's features and implementation needs.
- Project Managers: To oversee project planning, timelines, and deliverables.
- Quality Assurance (QA) Testers: To verify that all requirements are implemented correctly and reliably.
- Parents or Guardians (Stakeholders): To review the features they will have access to, ensuring it meets their expectations for protecting children.

Reading Recommendations:

- For a broad overview of the system: See Section 2 – Overall Description.
- For technical implementation details: Refer to Section 4 – System Features.
- For performance, safety, and other quality aspects: Review Section 5 – Non-Functional Requirements.

1.4 Product Scope

The Parental Control System is designed to help guardians manage and monitor how children use digital devices. The system enables users to:

- Block or filter access to inappropriate or harmful online content.
- Set time-based usage limits on devices or specific applications.
- Restrict device usage to only approved or safe applications/software.
- Monitor and report on activity logs and, when enabled, track device location.

By incorporating all four key areas of parental control—content filtering, usage controls, application management, and activity monitoring—the product aims to create a safer and healthier digital experience for children while giving parents peace of mind.

1.5 References

This document is informed by:

- Research on parental control best practices, trends, and tools.
- Industry standards for digital safety, filtering technologies, and child protection (e.g., ICRA, PEGI).
- Legal regulations and compliance frameworks related to child data privacy and online safety (e.g., COPPA, GDPR-K, and regional child safety acts).
- Sample SRS Document

2. Overall Description

2.1 Product Perspective

The Parental Control System is a standalone application or software module that integrates with digital televisions, computers, video games, mobile devices, and related software platforms.
It acts as a control layer between the child and the content or device, allowing parents to manage and restrict what the child can access or do.
This product can work independently or integrate with existing device settings or third-party software ecosystems.

2.2 Product Functions

The main functions of the Parental Control System include:
* Content Filtering → restrict access to inappropriate websites, apps, or media.
* Usage Controls → set time limits or block device usage during certain hours (e.g., bedtime or homework time).
* Computer Usage Management → enforce the use of only approved software or applications.
* Monitoring Tools → track activity history, browsing habits, app usage, and even device location.
* Reporting → send reports or notifications to parents about their child's activity.

2.3 User Classes and Characteristics

The parental control system serves three main types of users:

❖ Parents:

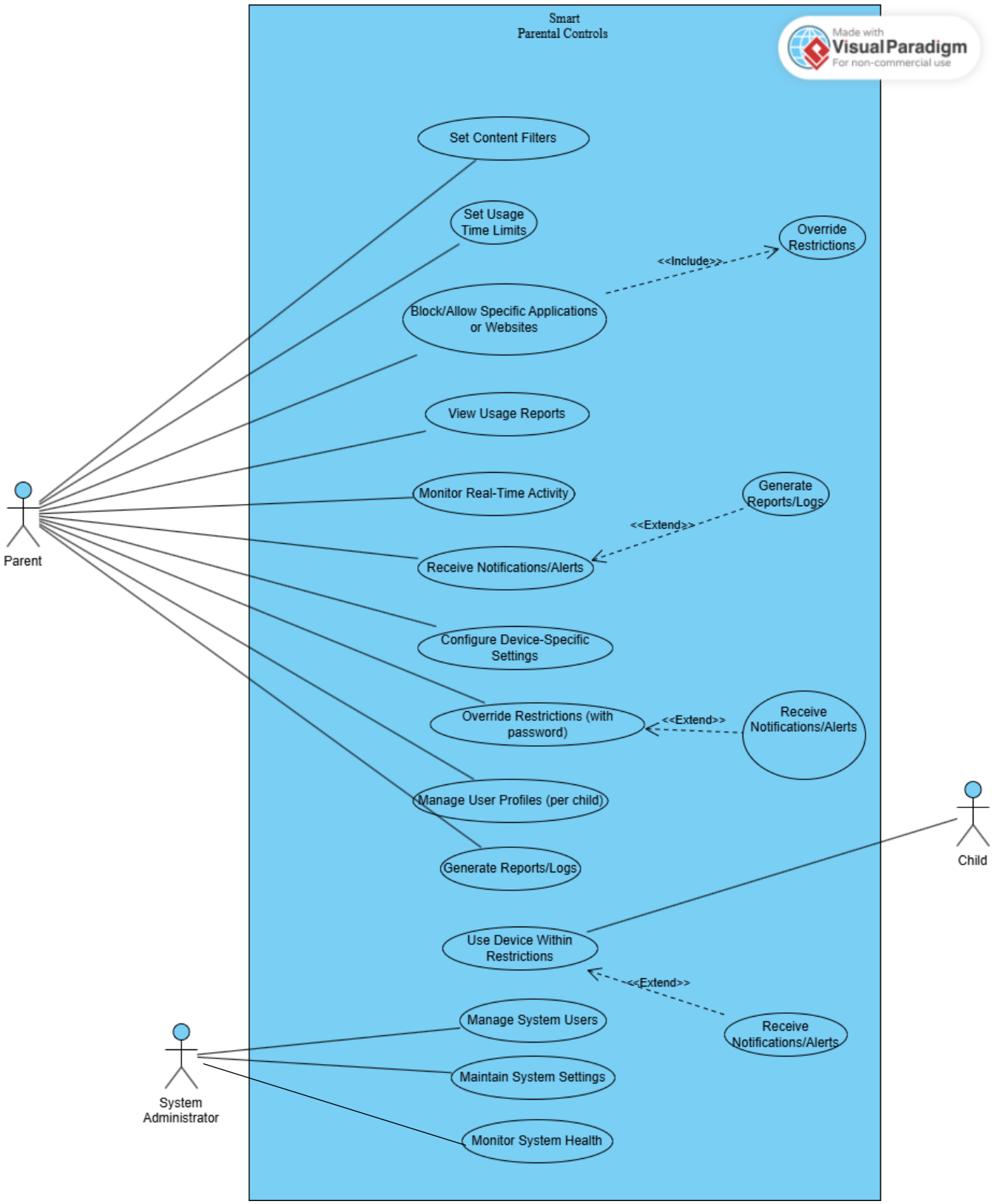
- Primary users of the system.
- Set up filters, time limits, monitoring, and receiving reports.
- Manage user profiles for each child.
- Can override restrictions when needed (using a password or PIN).
- Expect an easy-to-use, secure interface with clear notifications.

❖ Children/Users:

- Device users who are subject to parental controls.
- Can use devices within allowed limits and may receive notifications (e.g., when time is up or a blocked app is accessed).
- Typically, they have no access to system settings but may have limited options (like requesting more time).

❖ System Administrators (optional, backend role):

- Manage system-wide settings, user account creation, system maintenance, and updates.
- Ensure the system runs smoothly and securely.


Smart
Parental Controls
Made with
Visual Paradigm
For non-commercial use
Set Content Filters
Set Usage
Time Limits
Override
Restrictions
<<Include>>
Block/Allow Specific Applications
or Websites
View Usage Reports
Monitor Real-Time Activity
Generate
Reports/Logs
<<Extend>>
Receive Notifications/Alerts
Configure Device-Specific
Settings
Override Restrictions (with
password)
<<Extend>>
Receive
Notifications/Alerts
Manage User Profiles (per child)
Generate Reports/Logs
Use Device Within
Restrictions
<<Extend>>
Receive
Notifications/Alerts
Manage System Users
Maintain System Settings
Monitor System Health
Parent
System
Administrator
Child

•

2.4 Operating Environment

The system will run on:

- Mobile platforms → Android, iOS smartphones, tablets.
- Computers → Windows, macOS.
- Televisions or streaming devices → smart TVs, set-top boxes.
- Gaming consoles → PlayStation, Xbox, Nintendo Switch.

It should function reliably in environments with stable internet connections (for cloud-based monitoring) but also offer offline restrictions where possible.

2.5 Design and Implementation Constraints

Constraints include:

- Compliance with privacy laws (like COPPA, GDPR-K, or local child protection rules).
- Device compatibility limits (some older hardware may not support all features).
- Performance considerations (filtering and monitoring should not slow down device performance noticeably).
- Tamper resistance (the system must prevent children from easily bypassing controls).

2.6 User Documentation

Documentation will include:

- Quick start guides for setup.
- User manuals explaining all features in detail.
- FAQs and helpdesk contact info for troubleshooting.
- Online tutorials or videos for common tasks like setting time limits or viewing reports.

2.7 Assumptions and Dependencies

The system assumes:

- Parents have access to the devices they want to control.
- Devices have compatible operating systems and meet minimum hardware requirements.
- Users have internet access for cloud-based features like remote monitoring or reporting.
- Any third-party integrations (such as with smart TVs or game consoles) will provide API access or necessary permissions for the parental control software to function.

3. External Interface Requirements

3.1 User Interfaces

The parental control system will feature two types of user interfaces:

Parent-Facing Interface

This is the main control dashboard accessible via web, desktop, or mobile application, allowing parents or guardians to:

- Set content filters by age, content category, or specific websites/apps.
- Configure usage controls, including time limits and restricted usage periods.
- Approve or block the use of specific software/applications.
- Access activity logs, monitoring reports, and location data (if enabled).

Design Considerations:

- Interface must be intuitive and user-friendly with step-by-step guidance.
- Secure access is mandatory via PIN, password, or biometric authentication.
- Dashboard should offer clear visual indicators (e.g., charts, notifications) for ease of use.

Child-Facing Interface (Optional)

This lightweight interface may appear depending on the device type and configuration. Features include:

- Pop-up notifications (e.g., "Time almost up", or "This content is blocked").
- Simple, age-appropriate messages explaining restrictions.
- Non-intrusive design, ensuring it does not disrupt legitimate use.

3.2 Hardware Interfaces

The parental control system will interface with the following hardware platforms:

- Mobile Devices (smartphones, tablets):
    - Through OS-level access (Android/iOS) for enforcing restrictions.
- Personal Computers (Windows/macOS):
    - Integration via system hooks for software control and web filtering.
- Smart TVs and Streaming Devices:
    - Managed through available APIs or network/device-level controls.
- Game Consoles (e.g., PlayStation, Xbox, Nintendo):
    - Where APIs allow, the system may restrict usage or apply filters.

3.3 Software Interfaces

The system will integrate with a range of software components and services:

- Operating Systems: Android, iOS, Windows, macOS – for enforcing device-level controls.
- Third-Party Apps: Allow/block access to specific applications (where API access is granted).
- Web Browsers: Use of extensions or browser hooks to filter inappropriate content.
- Cloud Services: Enable centralized management of rules, remote updates, and multi-device sync.

All integrations must:

- Use secure and well-documented APIs.
- Respect system-level permissions and user consent.
- Be regularly updated for compatibility with OS updates.

3.4 Communications Interfaces

The parental control system requires reliable and secure communication channels:

- Internet Access:
    - For remote control, syncing settings, generating usage reports, and downloading updates.
- Local Network Communication:
    - For managing multiple devices connected to the same home Wi-Fi (e.g., smart TVs, routers).
- Cloud Connectivity:
    - For storing user preferences, managing accounts, and sending parental alerts across devices.

Security Requirements:

- All communication must use encrypted protocols (e.g., HTTPS, TLS/SSL).
- Personal data, such as child activity logs and settings, must be transmitted and stored securely and privately in accordance with data protection laws.

4.System Features(Functional Requirements)

4.1 Content Filtering

- As a parent,
  I can block access to specific websites, apps, or services based on categories like adult content, violence, or gambling,
  so that my child is only exposed to age-appropriate material.
- As a parent,
  I can apply age-based ratings (e.g., PG, 13+, 18+) across platforms,
  so that I maintain control over what content is suitable for each child.
- As a parent,
  I can enable safe search on supported browsers and platforms,
  so that search results are filtered for inappropriate content.
- As a parent,
  I can allow or block specific streaming services or individual videos,
  so that I can tailor the digital experience for my child's maturity level.

4.2 Usage Time Management

- As a parent,
  I can set daily or weekly screen time limits for my child,
  so that I encourage healthy device usage habits.
- As a parent,
  I can define periods (e.g., bedtime or homework time) when access to devices or specific apps is restricted,
  so that my child can focus on non-digital activities when needed.
- As a parent,
  I can receive notifications when screen time is about to expire,
  so that I stay informed and can manage expectations.
- As a parent,
  I can temporarily extend screen time as a reward,
  so that I can positively reinforce good behavior.

4.3 Activity Monitoring and Reporting

- As a parent,
  I can view my child's browsing and app usage history,
  so that I can have informed discussions about their online habits.
- As a parent,
  I can track my child's real-time location via mobile devices,
  so that I can ensure their safety when they are outside.
- As a parent,
  I can receive alerts when my child attempts to access blocked content,
  so that I am immediately aware of potential issues.
- As a parent,
  I can receive daily or weekly reports of my child's digital activities,
  so that I stay updated on their usage patterns.

4.4 Software Usage Control

- As a parent,
  I can restrict access to specific software or apps,
  so that my child only uses tools that support learning and development.
- As a parent,
  I can block the installation of new apps without my approval,
  so that I maintain control over what is installed on the device.

4.5 Tamper Protection

- As a parent,
  I can receive alerts if my child tries to disable or bypass the controls,
  so that I can respond promptly to maintain protection.
- As a parent,
  I can prevent the uninstallation or modification of the parental control system without my credentials,
  so that the system remains effective and secure.

4.6 Remote Management

- As a parent,
  I can manage all parental control settings remotely via a mobile app or web dashboard,
  so that I can monitor and adjust rules even when away from home.
- As a parent,
  I can apply rule changes instantly across all registered devices,
  so that I ensure consistent control regardless of location.

4.7 Multi-Profile Support

- As a parent,
  I can create separate profiles for each child,
  so that I can apply age-appropriate controls tailored to each one.
- As a parent,
  I can switch between profiles easily,
  so that each child has a personalized experience based on their needs.

4.8 Additional Feature: Emergency Access

- As a parent,
  I can set emergency contacts and apps to always be accessible,
  so that my child can reach help during critical situations.

5. Nonfunctional Requirements

5.1 Performance Requirements

- As a parent,
  I can apply content filtering with no noticeable delay,
  so that inappropriate content is blocked instantly and my child is protected in real time.
- As a parent,
  I can manage and monitor multiple child profiles simultaneously,
  so that the system remains efficient and responsive even with multiple users.
- As a parent,
  I can receive activity updates in real time or near real time,
  so that I can make quick and informed decisions regarding my child's device usage.
- As a user,
  I can generate usage or activity reports within a few seconds,
  so that I can quickly analyze behavior patterns without long wait times.

5.2 Safety Requirements

- As a parent,
  I can override restrictions instantly in emergencies,
  so that my child is not locked out from accessing help or essential services.
- As a parent,
  I can trust that emergency services and critical contacts are always accessible,
  so that my child's safety is not compromised by strict controls.
- As a guardian,
  I can ensure location tracking respects privacy settings and is only visible to authorized users,
  so that sensitive information about my child remains protected.

5.3 Security Requirements

- As a parent,
  I can secure parental controls with passwords, PINs, or biometric verification,
  so that my child cannot tamper with or disable the controls.

- As a system administrator,
  I can rely on encrypted storage and transmission of sensitive data,
  so that my child's activity logs and location data remain secure from unauthorized access.
- As a parent,
  I can receive alerts about failed login attempts or suspicious activity,
  so that I can take immediate action to protect the system and its data.

5.4 Software Quality Attributes

- As a parent,
  I can use an intuitive and user-friendly interface,
  so that I can configure settings without needing technical expertise.
- As a user,
  I can rely on the system maintaining at least 99.9% uptime,
  so that parental controls are enforced consistently without disruption.
- As a system maintainer,
  I can apply software updates easily,
  so that the system stays current and secure without full reinstallation.
- As a parent,
  I can scale the system across various platforms and devices,
  so that I can protect all my child's devices with a unified solution.

5.5 Business Rules

- As a verified parent,
  I can access and manage control features only after identity verification,
  so that unauthorized users are prevented from modifying settings.
- As a basic plan user,
  I can access essential features like filtering and time limits,
  so that I can protect my child without paying for a premium plan.
- As a premium user,
  I can access advanced features like remote management and detailed reporting,
  so that I get enhanced control and insights into my child's activity.
- As a parent,
  I can activate monitoring features only after giving informed consent,

so that the system complies with privacy and child protection regulations (e.g., COPPA, GDPR-K).

- As a parent,
  I must provide consent before activating tracking,
  so that my child's location is monitored responsibly.

❖ Additional Optional Features

- As a visually impaired parent,
  I can use the system with accessibility tools,
  so that I can protect my child without barriers.
- As a non-English speaker,
  I can use the app in my local language,
  so that it's easier to navigate and configure.

6. Other Requirements

- Multi-child profile management
  Parents can create and manage multiple child profiles with separate settings for each child.
- Blocked content notifications
  Parents receive alerts when a child tries to access restricted content.
- Device compatibility
  Works on smartphones, tablets, PCs, and smart TVs.
- Activity reports
  Shows reports on screen time, app usage, and child location (if supported).
- Tamper resistance
  Continues to work even if the child tries to disable or uninstall it.

➢ Additional Requirements

- Legal compliance
  Follows regulations like:
  - COPPA (Children's Online Privacy Protection Act)

- GDPR-K (General Data Protection Regulation – Kids)

- Third-party integration
  Can connect with:
  - YouTube Kids
  - Educational apps and platforms
- Multilingual and regional filtering
  Supports different languages and filters content based on the region.
- Backup and restore
  Parental settings can be saved and restored across devices.
- Optional integrations
  May support:
  - School systems for syncing academic restrictions
  - Wearable devices for tracking and alerts

Appendix A: Glossary

- Parental Controls - Features that help parents limit or monitor their child's digital activity.
- Content Filters - Blocks websites, apps, or videos not suitable for children.
- Usage Controls - Sets limits on how long or when devices can be used.
- Monitoring - Tracks what children do on their devices.
- Child Profile - A customized account for each child.
- Geofencing - Sends alerts when a child enters or exits a specific area.
- PIN/Password Lock - Protects settings so children cannot change them.

Appendix B: Analysis Models

This section includes diagrams or models that help explain system behavior or structure.

For parental controls, you can include:

- Use Case Diagrams: Showing how parents, children, and the system interact.

- Activity Diagrams: Showing the flow of actions, e.g., when a parent sets up a new filter.
- Sequence Diagrams: Showing interactions over time, e.g., when a child tries to access a blocked site and the system responds.
- Data Flow Diagrams: Showing how data (like activity logs) moves through the system.
- Wireframe Structure: A wireframe is a low-fidelity visual blueprint of your system's interface. It focuses on layout and functionality—not final design or colors.

1. Splash Screen

✓ App logo

✓ App name: " Smart Parental Controls "

2. Login / Sign Up Screen

✓ Email / Phone

✓ Password

✓ [Login] button

✓ [Sign Up] link

✓ [Forgot Password] link

3. Parent Dashboard

Main Navigation (Tabs or Drawer):

✓ Home

✓ Devices

✓ Screen Time

✓ Content Filter

✓ Reports

✓ Settings

✓ Dashboard Highlights:

✓ Child Profiles (Name, Age, Profile Pic)

- ✓ Device Status (Online/Offline)
- ✓ Quick Actions:
    - Lock Device
    - View Usage
    - Set Screen Time
    - Content Filters

4. Add Child Profile Screen

- ✓ Child Name
- ✓ Age
- ✓ Profile Photo Upload
- ✓ Device Link Code (for child's device)
- ✓ [Save] button

5. Screen Time Management

- ✓ Select Child
- ✓ Set daily screen time (slider or input)
- ✓ Schedule (Days & Time Ranges)
- ✓ [Apply] button

6. Content Filter Screen

- ✓ Select Child
- ✓ Categories:
    - Adult Content
    - Violence
    - Social Media
    - Games
- ✓ Toggle switches for each category
- ✓ Option to add custom blocked websites/apps
- ✓ [Save Settings] button

7. Activity Report Screen

- ✓ Select Child
- ✓ Today's Usage Summary
    - Total Screen Time
    - Most Used Apps
    - Blocked Content Attempts
- ✓ Option to export PDF report

8. Settings Screen

- ✓ Parent Account Info
- ✓ Change Password
- ✓ Add Admin/Guardian
- ✓ Notifications Preferences
- ✓ Help / Support
- ✓ Logout

Appendix C: To Be Determined (TBD) List

- ➢ Maximum number of child profiles - Decide how many profiles one parent can create.
- ➢ Language support - Confirm which languages the system will support.
- ➢ Integration with other platforms - Decide if the system will work with third-party apps (e.g., YouTube Kids).
- ➢ AI-based content detection - Confirm if the system will use AI to detect inappropriate content.
- ➢ Data storage method - Decide whether to use cloud or local storage for logs and reports.