1. Ethics & Privacy in Assistive Technology

Key Risks & Ethical Themes

- **Privacy & data protection**: Assistive technologies must ensure confidentiality, data integrity, availability, and accountability. Sensor footage (e.g., camera or location data) must be stored securely and protected against unauthorized access [SpringerLink](#).
- **Autonomy and human dignity**: Ethical frameworks (like WHO GATE, Kitchener's "Golden Five") emphasise supporting user autonomy, promoting dignity, avoiding social stigma, and preventing replacement of human care [SpringerLink+2Taylor & Francis Online+2ResearchGate+2](#).
- **Algorithmic bias & transparency**: Real-world studies warn of bias in AI models and a lack of legal/regulatory depth, urging transparent, bias-aware design [MDPIarXiv](#).

Contextual Constraints for Your Project

- In a **library setting**, visual/audio sensors may capture individuals without consent (e.g., CCTV, Wi-Fi tracking). You must consider Deakin's existing policies on surveillance and data logging [Deakin University](#).
- Device design must balance **usability, reliability, confidentiality**, and **freedom of choice** for users; avoid intrusive monitoring that might stigmatize users [SpringerLink+11SpringerLink+11iri.upc.edu+11](#).

2. Deakin Policies & Compliance

Surveillance & Data Collection

- **CCTV and location tracking**: Deakin uses fixed/floating cameras, Wi-Fi/device logging, building access systems. Data is used for security, space usage, and analytics—kept with access controls [Deakin University](#).

ICT Security & Privacy

- **ICT Security Policy** mandates protecting data from corruption/loss/unauthorised access with appropriate controls [policy.deakin.edu.au](#).
- **Privacy Policy** requires compliance with Victorian legislation and ensures personal info is gathered lawfully and destroyed per retention protocols [leadership.deakin.edu.au+1Deakin University+1](#).

3. Connecting Research to Project Context

Task	Finding	Relevance to Device
Sensor review	Identify privacy, bias, autonomy risks	Helps determine what to log, store, or anonymize
Deakin policy alignment	Focus on CCTV, Wi-Fi and access data	Use only data that aligns with existing protocols
Ethical design standards	Use VSD & privacy by design	Ensure ethics are integrated early in design arXiv+12Wikipedia+12SpringerLink+12help.deakin.edu.au+11Deakin University+11help.deakin.edu.au+11policy.deakin.edu.au+1Deakin University+1
Bias/transparent AI	Implement logging, user control options	Build trust and accountability into navigation feedback
Consent framework	Consider dynamic consent models	Enables users to modify permissions over time Wikipedia

4. Ethical Constraints for Design

- **Data minimisation**: Log only essential data keeping to library use cases Wikipedia.
- **Secure storage**: All sensor data must be encrypted and access-controlled SpringerLink.
- **User consent**: Use clear signage and dynamic consent for data capture Wikipedia.
- **Transparency**: Inform users about what data is captured, for what purpose, and how long it is stored.
- **Bias mitigation**: Test across diverse environments to ensure fair object detection.
- **Avoid stigma**: Ensure device feels empowering, not intrusive—support discretion.

5. Summary to Share

"This literature review examined ethics and privacy in assistive tech, focusing on user autonomy, confidentiality, and bias. We cross-referenced these with Deakin's privacy and ICT policies (covering CCTV, Wi-Fi tracking, data retention/security). For the library-based navigational device, we recommend:

1. Data minimisation: capture only what's essential in real time
2. Secure, access-controlled data handling (encrypt & limit retention)
3. Dynamic consent (user-controlled permission)
4. Clear disclosure to users about data use
5. Rigorous testing in diverse environments
6. Design that avoids making users feel surveilled or stigmatized