NutriLift

A Fitness and Nutrition Tracking Mobile Application with Community and Gamification Features

Academic Year	Module	Assessment Number	Assessment Type
2025/2026	Project and Professionalism	P2	Professionalism Report

Full Name: Luja Ratna Manandhar

Student Number: 2407087

Course: BSc. (Hons) Computer Science

University Email: L.R.Manandhar@wlv.ac.uk

Supervisor: Johan Tandukar

Reader: Yogesh Bikram Shah

Date of Submission: January, 2025

Abstract:

This report analyzes the professional aspects of NutriLift, a Flutter-based mobile fitness app with nutrition tracking, computer vision workouts, gamification, community features, and premium gym discovery. It evaluates social impacts (motivation benefits versus anxiety risks from leaderboards), ethical issues (consent transparency, health messaging, vulnerable user protections amid real-world misuse like harmful posts), legal compliance (UK GDPR for health data, Equality Act accessibility, IP rights, Nepal privacy laws), and security practices (bcrypt auth, TLS encryption, moderation against breaches). Drawing from development experience, the report demonstrates responsible engineering through risk mitigations, professional duty of care, and future scalability considerations for user wellbeing.

Table of Contents

1. Introduction

NutriLift is a mobile health and fitness application developed as a project to support users particularly university students and fitness beginners in establishing sustainable wellness habits through integrated nutrition tracking, workout logging, gamified motivation systems, and social community features. The application incorporates several core modules: personalised nutritional analysis with dietary logging; exercise tracking with computer vision-based repetition counting using the device camera; progress visualisation through charts and wellness metrics; gamified achievement systems with challenges and leaderboards; a moderated community feed for peer support; and premium subscription management with integrated gym discovery and membership tracking functionality.

This companion report examines the professional, ethical, legal, and security dimensions of NutriLift's design and development. As an application that influences user behaviour patterns, collects sensitive personal health data, and facilitates peer interaction within a community environment. NutriLift carries significant responsibilities beyond technical implementation. This analysis reflects the explicit requirements to consider the non-functional but critical aspects of software development in real-world contexts.

2. Social Impact

2.1. Positive Social Effects:

NutriLift is designed to generate positive social impact by removing barriers to health tracking and motivation. The application's nutrition and exercise logging systems provide users with structured data visualisation capabilities, enabling evidence-based monitoring of dietary and physical activity patterns. The progress dashboard module, featuring charts and aggregated wellness scores, supports user motivation through transparent feedback about effort and improvement trajectory. This is particularly beneficial for university students and fitness novices who may lack access to personalised coaching or structured gym environments (Lister, et al., 2014).

The gamification subsystem implemented through achievements, challenge streaks, and performance metrics aims to leverage established behavioural psychology principles to sustain engagement over extended periods. Research indicates that well-designed gamification can increase adherence to health behaviours by 20–30% and improve long-term motivation when structured appropriately (Johnson, et al., 2016). The community module extends this positive effect by enabling social support, with features allowing users to publicly celebrate milestones, exchange encouragement, and build accountability partnerships with peers. This peer-support function has been shown to reduce feelings of isolation in fitness pursuits and strengthen commitment to wellness goals, particularly among populations lacking traditional fitness community access (Alzghoul, 2024).

2.2. Potential Negative Social Effects and Mitigation Strategies:

However, the same features introduce risk of psychological harm if not implemented with care. Leaderboards and competitive challenge mechanics can exacerbate social comparison anxiety, particularly among users with pre-existing body image concerns or eating disorder vulnerabilities. Research into the "dark side" of gamified health applications demonstrates that poorly designed leaderboards and comparative metrics can trigger anxiety, reduce intrinsic motivation, and paradoxically decrease adherence over time through the "overjustification effect" whereby external rewards undermine internal motivation (Chen, et al., 2023). Additionally, emphasis on caloric reduction, weight tracking, or daily streaks may inadvertently reinforce unhealthy relationships with food and exercise in vulnerable populations.

To mitigate these risks, NutriLift's design employs several safeguards. Leaderboards emphasise personal progress over absolute ranking, using relative improvement metrics rather than comparative performance. Community guidelines explicitly prohibit body-shaming language and comparison-focused commentary. The application avoids punitive mechanics (e.g., loss of points for missed days) that could create anxiety; instead, broken streaks simply reset to zero, reducing shame-based engagement. Notification systems are designed to encourage, not pressure, through positive framing. Critically, the wellness score algorithm avoids prescriptive weight loss or restrictive dietary messaging, instead focusing on balanced nutrition and sustainable habits (International Journal of Environmental Research and Public Health, 2021).

3. Ethical Issues:

3.1. Informed Consent and Data Transparency:

NutriLift collects sensitive personal and health-related data during user registration and throughout the application lifecycle, including age, biological sex, height, weight, dietary preferences, meal composition details, exercise type and duration, location patterns (via gym discovery), and activity streaks. Under established ethical principles and regulatory frameworks, users must provide informed, specific consent for each distinct data processing purpose.

The application implements transparent consent mechanisms through multi-stage disclosure: a concise privacy statement at registration explaining primary data uses (personal progress tracking, nutrition analytics, workout recommendations); a dedicated privacy settings panel allowing granular control over community visibility and data sharing; and detailed in-app documentation describing the data flow through internal modules (e.g., the wellness score algorithm's use of dietary and activity data). Users retain meaningful control, including the ability to edit or delete log entries, mark themselves as private in the community module, and withdraw from challenge leaderboards without account deletion (Department of Health & Social Care, 2021).

3.2. Ethical Design and Health Messaging:

NutriLift must avoid reinforcing harmful health misconceptions or promoting extreme practices. The application explicitly disclaims provision of medical advice; all generated nutrition and fitness recommendations are explicitly framed as general wellness guidance rather than clinical recommendations. The application does not prescribe caloric targets without user-initiated personalisation, avoiding paternalistic diet enforcement. Importantly, language throughout the interface avoids moralistic framing ("bad" foods, "failure" to exercise); instead, all messaging uses neutral, progress-oriented terminology. The wellness score does not penalise weight gain or plateaued weight loss, instead measuring consistency and balance across nutritional and activity dimensions.

The community module presents particular ethical challenges. User-generated content (posts, comments, advice) may propagate dangerous health misinformation or body-shaming rhetoric. NutriLift addresses this through:

(1) automated content flagging for medical claims, extreme dieting advice, and body-critical language;
(2) community guidelines explicitly prohibiting harassment, disordered eating promotion, and discrimination;
(3) user-facing reporting mechanisms for harmful content;
(4) admin moderation with authority to remove non-compliant posts and suspend repeat offenders.

3.3. User Autonomy and Vulnerability Protections:

Ethical data processing requires protecting user autonomy, particularly for vulnerable populations (users with eating disorders, body dysmorphic disorder, or mental health conditions). While NutriLift cannot screen users, the design minimises exploitation risk through transparent opt-in mechanisms for social features (not pre-enabled), privacy defaults favouring data minimisation (community posts are private unless explicitly shared), and prominent in-app signposting of mental health and eating disorder support resources. The application includes a voluntary "anonymous logging" mode for users who wish to track privately without community exposure (Department of Health & Social Care, 2021).

Despite these safeguards, real-world use introduces risks that design alone cannot eliminate. For instance, a user might post subtle pro-anorexia content using coded language that automated filters miss. A volunteer moderator however well-intentioned might lack clinical training to recognise distress or may delay action due to oversight. In such cases, harmful content could remain visible during critical moments, potentially triggering vulnerable peers. This highlights that ethical responsibility doesn’t end at launch; it requires ongoing investment in moderation quality, user reporting responsiveness, and partnerships with mental health experts to handle edge cases effectively.

4. Legal Implications

4.1. Data Protection and GDPR Compliance

The United Kingdom’s Data Protection Act 2018 (implementing the UK General Data Protection Regulation) establishes the legal framework governing NutriLift’s data collection and processing. Under UK GDPR Article 6, NutriLift must establish a lawful basis before processing any personal data. For NutriLift, the appropriate basis is Article 6(1)(a) explicit user consent since the application provides personalised wellness services rather than fulfilling legal obligations. Critically, health-related data constitutes "special category personal data" under Article 9 of UK GDPR, necessitating additional safeguards including explicit, affirmative consent obtained separately from general terms of service and clear explanation of data processing purposes (UK Government, 2018) ((ICO), 2023).

NutriLift complies through a mandatory, standalone consent interface during registration, explicit listing of health data processing operations, accessible privacy policy documentation, and robust backend encryption. Users retain comprehensive data subject rights under Articles 15–22 of UK GDPR, including rights of access, rectification, erasure ("right to be forgotten"), restriction of processing, and objection.

4.2. Equality and Non-Discrimination:

The Equality Act 2010 prohibits discrimination in the provision of services on the basis of protected characteristics (UK Government, 2010). NutriLift ensures compliance by:

(1) Following WCAG 2.1 Level AA accessibility standards (high contrast, screen reader support, keyboard navigation);

(2) Using inclusive imagery and avoiding stereotyping;

(3) Auditing the wellness algorithm for bias (e.g., exercise suggestions are not gender-filtered);

(4) Supporting diverse user needs, including mobility constraints and cultural dietary practices (Level Access, 2025).

4.3. Intellectual Property and Content Rights:

All external content (exercise descriptions, nutritional data, icons) is either original, properly licensed, or sourced from open databases (e.g., UK Food Standards Agency) with attribution. No proprietary content is used without permission. For user-generated content, NutriLift's terms of service grant users full copyright while providing the platform a non-exclusive licence to display and moderate protecting both user rights and operational integrity (UK Intellectual Property Office, 2023).

4.4. Payment Processing and Regulatory Compliance:

Premium subscriptions are processed via certified third parties (e.g., Stripe, Apple App Store), ensuring compliance with PCI DSS v4.0 (Payment Card Industry Security Standards Council, 2024). NutriLift never handles raw card data; only 6okenized identifiers are stored for subscription validation (Payment Card Industry Security Standards Council, 2024).

Compliance with GDPR, the Equality Act, and PCI DSS isn't merely about avoiding fines it's about upholding user dignity and autonomy. For example, treating health data as "special category" under UK GDPR acknowledges its sensitivity and the potential for misuse if exposed. Similarly, designing for accessibility isn't just legal compliance; it's a commitment to inclusive service provision. These choices signal that NutriLift prioritises user rights over convenience, which is central to professional conduct in digital health.

4.5. Nepal-Specific Legal Aspect: Right to Privacy and Consumer Protection

Nepal's Constitution, 2072 (2015), constitutionally guarantees the right to privacy in Article 28, which protects privacy relating to the person, residence, property, documents, data, correspondence, and character from arbitrary interference, except as permitted by law (Government of Nepal, 2015). NutriLift, if it serves users in Nepal or processes data of Nepali citizens, must therefore comply with Nepal's data protection framework, primarily the Privacy Act, 2075 (2018). Under this Act, explicit, informed consent must be obtained before collecting personal or health data, and data use must be limited to clearly defined purposes with adequate security safeguards (Government of Nepal, 2018).

Additionally, the Consumer Protection Act, 2075 (2018) requires that digital services provide clear information about terms, pricing, and consumer rights, and that unfair trade practices and insecure handling of consumer data are prohibited (Nepal, 2018). NutriLift's local operations in Nepal must ensure transparent disclosures, fair cancellation and refund policies, and accessible mechanisms for complaint resolution, aligning with both Nepali consumer rights and international best practices in digital health apps.

5. Security Aspects

5.1. User Authentication and Access Control:

Passwords are hashed using bcrypt with unique salts. Optional multi-factor authentication (MFA) is available. Authentication tokens expire after 24 hours. Role-based access control (RBAC) enforces least privilege: standard users access only their own data; moderators access flagged content only; administrators access operational metrics without blanket health data access ((NIST), 2017) (OWASP Foundation, 2025).

5.2. Data Protection in Transit and at Rest:

All communication uses TLS 1.3 (minimum TLS 1.2). Certificate pinning prevents man-in-the-middle attacks. Sensitive data at rest is encrypted using AES-256, with keys managed via a dedicated key management service (KMS). Password hashes are salted and stretched to resist brute-force attacks.

5.3. Input Validation and Attack Prevention:

All inputs undergo server-side validation. Database queries use parameterised statements to prevent SQL injection. Community content is sanitised to block XSS. Rate limiting protects against brute-force and spam attacks.

5.4. Logging, Monitoring, and Incident Response:

Security-relevant events (logins, data access, moderation actions) are logged in tamper-resistant formats. Anomalous activity triggers alerts. In case of a breach, NutriLift follows a GDPR-aligned incident response plan: containment, investigation, user notification (if high risk), and ICO reporting within 72 hours.

5.5. Third-Party Security:

Third-party providers (cloud, payments, analytics) are selected based on ISO 27001 or SOC 2 certification. Data Processing Addendums (DPAs) comply with UK GDPR Article 28. Only necessary, anonymised data is shared with analytics partners (UK Government, 2018)

These security measures reflect not only technical best practices but also a professional duty of care. Handling sensitive health data such as dietary logs, workout habits, and body metrics means that any breach could cause real psychological or social harm, especially for vulnerable users. Choosing bcrypt over weaker hashing, enforcing TLS 1.3, and avoiding direct handling of payment data aren't just engineering choices; they demonstrate accountability to users who place trust in the system. As future professionals, developers must recognise that robust security is an ethical baseline, not an optional feature.

6. Conclusion:

Developing NutriLift has reinforced the principle that responsible software engineering extends beyond functional correctness to encompass profound ethical, legal, and social dimensions. The application's design choices in social gamification, data transparency, non-discriminatory accessibility, privacy-by-design architecture, and security controls reflect deliberate reflection on professional obligations to users.

Social impact analysis revealed opportunities to motivate behaviour change whilst mitigating risks of comparison anxiety and unhealthy obsession through design that emphasises personal progress, avoids shame-based language, and supports vulnerable users. Ethical examination established that clear informed consent, transparent data use, respectful community governance, and alignment with established health communication principles are non-negotiable. Legal and security implementations grounded in GDPR, Equality Act, and industry standards protect user rights and data integrity as foundational responsibilities, not afterthoughts.

That said, professional maturity also means acknowledging limitations. Scaling human moderation affordably while maintaining response quality remains a challenge as user numbers grow. Long-term support for at-risk users beyond static resource links may require integration with clinical services or AI-assisted risk detection trained on public health guidelines. Future iterations should explore these pathways to ensure NutriLift evolves not just in features, but in its capacity to safeguard wellbeing responsibly. As personal health increasingly moves into digital spaces, developers must meet rising expectations of care, vigilance, and humility.

References

(ICO), I. C. O., 2023. *UK GDPR guidance: Individual rights.* [Online]
Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/
[Accessed 23 January 2026].

(NIST), N. I. o. S. a. T., 2017. *Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management,* Gaithersburg, MD: National Institute of Standards and Technology.

Alzghoul, B., 2024. The Effectiveness of Gamification in Changing Health-related Behaviors: A Systematic Review and Meta-analysis. *The Open Public Health Journal,* 06 September.p. e18749445234806.

Arora, C. & Razavian, M., n.d. Ethics of Gamification in Health and Fitness-Tracking. *International Journal of Environmental Research and Public Health,* 18(21), p. 11052.

Chen, H., Schoefer, . K., Manika, D. & Tzemou, E., 2023. The "Dark Side" of General Health and Fitness-Related Self-Service Technologies: A Systematic Review of the Literature and Directions for Future Research. *Journal of Public Policy & Marketing,* 13(2), p. 121–138.

Department of Health & Social Care, 2021. *Data security and protection toolkit: Guidance for health and social care organisations.* [Online]
Available at: https://www.dsptoolkit.nhs.uk
[Accessed 23 January 2026].

Government of Nepal, 2015. *The Constitution of Nepal, 2072 (2015).* [Online]
[Accessed 23 January 2026].

Government of Nepal, 2018. *The Privacy Act, 2075 (2018).* [Online]
[Accessed 23 January 2026].

Johnson, D. et al., 2016. Gamification for health and wellbeing: A systematic review of the literature. *Internet Interventions,* Volume 6, pp. 89-106.

Level Access, 2025. *Equality Act 2010 and UK web accessibility laws: Compliance guide.* [Online]
Available at: https://www.levelaccess.com/blog/united-kingdom-accessibility-requirements
[Accessed 23 January 2026].

Lister, C. et al., 2014. Just a fad? Gamification in health and fitness apps. *JMIR Serious Games,* 2(2), p. e9.

Nepal, G. o., 2018. *The Consumer Protection Act, 2075 (2018).* [Online]
[Accessed 23 January 2026].

OWASP Foundation, 2025. *OWASP Mobile Top 10.* [Online]
Available at: https://owasp.org/www-project-mobile-top-10
[Accessed 23 January 2026].

Payment Card Industry Security Standards Council, 2024. *PCI DSS Version 4.0 Requirements and Assessment Procedures,* s.l.: PCI Security Standards Council.

UK Government, 2010. *Equality Act 2010.* [Online]
Available at: https://www.legislation.gov.uk/ukpga/2010/15
[Accessed 23 January 2026].

UK Government, 2018. *Data Protection Act 2018.* [Online]
Available at: https://www.legislation.gov.uk/ukpga/2018/12
[Accessed 23 January 2026].

UK Intellectual Property Office, 2023. *Intellectual property: Your rights.* [Online]
Available at: https://www.gov.uk/guidance/intellectual-property
[Accessed 23 January 2026].