**Proposal For Health Advice Group**

**Table Of Contents**

Table of Contents

[Organisation Overview 4](#_Toc188527031)

[Business Description 4](#_Toc188527032)

[Problem Overview 4](#_Toc188527033)

[User Groups 4](#_Toc188527034)

[Empathy Map 4](#_Toc188527035)

[Users 4](#_Toc188527036)

[User Stories 4](#_Toc188527037)

[Laws, Guidance, Legislations and Standards 5](#_Toc188527038)

[1. Laws 5](#_Toc188527039)

[Data Protection Act 2018 (DPA 2018) 5](#_Toc188527040)

[2. Legislation 5](#_Toc188527041)

[Network and Information Systems Regulations 2018 (NIS Regulations) 5](#_Toc188527042)

[Telecommunications (Data Protection and Privacy) Regulations 2000 6](#_Toc188527043)

[Shape 3. Guidelines 6](#_Toc188527044)

[ICO Guidelines on Data Protection 6](#_Toc188527045)

[Web Content Accessibility Guidelines (WCAG) 6](#_Toc188527046)

[4. Standards 7](#_Toc188527047)

[ISO/IEC 27001:2013 (Information Security Management System - ISMS) 7](#_Toc188527048)

[Cyber Essentials 7](#_Toc188527049)

[Alternative Systems 7](#_Toc188527050)

[1. Defra Air Quality Index 7](#_Toc188527051)

[2. BBC Weather 8](#_Toc188527052)

[3. Allergy UK Pollen Count 8](#_Toc188527053)

[4. Air Quality Index UK (Air Quality Egg) 8](#_Toc188527054)

[5. Pollen Count UK (UK Pollen Count) 9](#_Toc188527055)

[Risks 9](#_Toc188527056)

[1. Unauthorized Access to Sensitive Data 9](#_Toc188527057)

[2. Weak Passwords or Compromised Accounts 10](#_Toc188527058)

[3. Data Breaches or Leaks 10](#_Toc188527059)

[4. Phishing or Social Engineering Attacks 10](#_Toc188527060)

[5. System Downtime or Denial of Service (DoS) Attacks 10](#_Toc188527061)

[Decomposition 10](#_Toc188527062)

[Diagram 10](#_Toc188527063)

[Description 10](#_Toc188527064)

[User Acceptance Criteria 11](#_Toc188527065)

[Functional And Non-Functional Requirements 11](#_Toc188527066)

[Functional Requirements 11](#_Toc188527067)

[Definition of a Functional Requirement 11](#_Toc188527068)

[1.Registration 11](#_Toc188527069)

[1.1 What Details Will be used to sign up 11](#_Toc188527070)

[1.2 Password Requirements 11](#_Toc188527071)

[1.4 Login 12](#_Toc188527072)

[Non-Functional Requirements 12](#_Toc188527073)

[2.1 Definition of a Non-Functional Requirement 12](#_Toc188527074)

[2.2 Efficient Loading Times 12](#_Toc188527075)

[2.3 Secure Password Storage 12](#_Toc188527076)

[2.4 Secure Data Storage 13](#_Toc188527077)

[Key Performance Indicators 13](#_Toc188527078)

# Organisation Overview

## Business Description

The Development company I work for are contracted to a company called Health Advice Group (HAG), they are a charity that offers information and support around environmental health issues. They are wanting a product developed to provide weather forecasting to users alongside relevant healthcare advice, A dashboard for monitoring air quality of a location and advice on how to deal with health conditions influenced by weather and other environmental conditions.

## Problem Overview

As I understand it, the problem HAG faces is that they either have an abhorrently out of date system OR just no digital solution at all, this of course means that the charity is incredibly limited in what they can do and their market catchment area / reach.

Specific examples for issues the

## User Groups

Business Administrator - Management

Everyday Service User – From Doris the doll (elderly ) to Gerald the geographer ( hiking etc) to standard sally (everyone else)

Everyday Staff - Developers etc.

### Empathy Map

#### Users

|  |  |
| --- | --- |
| **Says**   * I want to be able to read |  |
|  |  |

## User Stories

|  |  |  |  |
| --- | --- | --- | --- |
| As a [role] | I want … | So that … | Acceptance Criteria |
|  |  |  |  |

# Laws, Guidance, Legislations and Standards

Given that this project seems UK based I am going to assume that the laws that need to be abided by are the laws of UK.

## 1. Laws

These are overarching legal statutes passed by the UK Parliament that dictate how data must be managed and secured in various contexts.

### Data Protection Act 2018 (DPA 2018)

* **Overview**: Governs the processing of personal data in the UK and implements the **General Data Protection Regulation (GDPR)** into UK law.
* **Key Provisions**:
* **Lawful Basis for Processing**: Data must be processed lawfully and transparently.
* **Data Subject Rights**: Individuals have rights to access, correct, and request deletion of their data.
* **Data Protection by Design and Default**: Privacy must be integrated into the design of the project.

## 2. Legislation

Legislation refers to legal frameworks or specific regulatory acts that complement or enforce broader laws. These regulations ensure compliance with specific industry requirements, especially regarding cybersecurity and data protection.

### Network and Information Systems Regulations 2018 (NIS Regulations)

* **Overview**: Aims to improve the cybersecurity resilience of organizations providing essential services (e.g., education, healthcare).
* **Key Provisions**:
* **Security Requirements**: Ensures organizations take steps to secure their information systems.
* **Incident Notification**: Organizations must notify authorities in case of a major disruption.
* **Risk Management**: Requires adoption of risk management practices to secure critical infrastructure.

### Telecommunications (Data Protection and Privacy) Regulations 2000

* **Overview**: These regulations relate to privacy and data protection in telecommunications and internet services.
* **Key Provisions**:
* **Privacy of Communications**: Ensures privacy of user data and communications.
* **Security**: Mandates appropriate security measures for networks handling personal data.

## Shape 3. Guidelines

These are advisory documents from regulatory bodies that provide detailed recommendations for organizations to ensure compliance with laws and standards.

### ICO Guidelines on Data Protection

* **Overview**: The Information Commissioner’s Office (ICO) provides detailed guidance on how organizations should process personal data in compliance with the DPA 2018 and GDPR.
* **Key Provisions**:
* **Transparency**: Requires clear communication about data collection, usage, and storage practices.
* **Data Security**: Encourages strong data protection practices, including encryption and secure storage.
* **Rights of Individuals**: Specifies how organizations should manage data access and correction requests from individuals.

### Web Content Accessibility Guidelines (WCAG)

* **Overview**: These guidelines ensure that digital platforms are accessible to users with disabilities.
* **Key Provisions**:
* **Text Alternatives**: Ensures that all images and non-text content have descriptive text equivalents.
* **Keyboard Accessibility**: Ensures users can navigate content using a keyboard alone.
* **Colour Contrast**: Provides requirements for readable colour contrasts for users with visual impairments.

## 4. Standards

These are detailed, internationally recognized frameworks that help organizations implement best practices in data protection and cybersecurity.

### ISO/IEC 27001:2013 (Information Security Management System - ISMS)

* **Overview**: ISO 27001 provides a systematic approach to managing sensitive company information and ensuring its security.
* **Key Provisions**:
* **Risk Assessment and Management**: Identifies and addresses information security risks.
* **Security Controls**: Implements policies for access control, encryption, and incident response.
* **Audit and Review**: Organizations must perform regular audits to assess the effectiveness of their information security systems.

### Cyber Essentials

* **Overview**: A UK government-backed cybersecurity certification scheme that sets out basic security controls to protect against common cyber threats.
* **Key Provisions**:
* **Security Controls**: Ensures the implementation of essential security measures such as secure configurations and malware protection.
* **Certification Levels**: Includes basic **Cyber Essentials** and more rigorous **Cyber Essentials Plus**.
* **Incident Management**: Requires a clear response plan for cybersecurity incidents.

# Alternative Systems

## 1. Defra Air Quality Index

* **Website**: uk-air.defra.gov.uk
* **Features**: Provides detailed air quality data for multiple UK locations, with real-time monitoring of pollutants like PM2.5, NO2, ozone, and more.
* **Downsides**:
  + **No Mobile App**: While the website is mobile-friendly, there's no standalone app for on-the-go access.
  + **Complex Interface**: The website can be a bit technical, which might be overwhelming for users who just want a quick overview.
  + **Limited Pollen Info**: Focuses mainly on-air quality; doesn’t provide detailed pollen or UV data.

## 2. BBC Weather

* **Website**: bbc.co.uk/weather
* **App**: BBC Weather app (available for iOS and Android)
* **Features**: Comprehensive weather forecasts, UV index, and pollen count data for various locations.
* **Downsides**:
  + **Pollen Forecast is Basic**: The pollen data is not as detailed as other services (e.g., specific types of pollen).
  + **Limited Air Quality Data**: While it gives a general idea of UV levels and weather conditions, it doesn't go deep into air quality or provide real-time pollutant data like some dedicated air quality apps.
  + **General Focus**: The app is focused more on weather and less on health-related factors like air pollution or allergens.

## 3. Allergy UK Pollen Count

* **Website**: [allergyuk.org](https://www.allergyuk.org)
* **Features**: Provides pollen forecasts, including tree, grass, and weed pollen levels across the UK. Offers general allergy-related advice.
* **Downsides**:
  + **No Dedicated App**: While the website is mobile-friendly, there's no specific app for easier access.
  + **Limited Data**: The site doesn’t cover air quality or UV levels in detail. Its focus is almost entirely on pollen counts and allergies.
  + **Region-Specific Data**: While it offers broad UK data, the pollen count might not always be localized enough for more specific areas.

## 4. Air Quality Index UK (Air Quality Egg)

* **Website**: [airqualityegg.com](https://www.airqualityegg.com)
* **Features**: Provides real-time air quality data, including pollutants like particulate matter (PM), nitrogen dioxide (NO2), and ozone. It also tracks pollen levels and UV index in some areas.
* **Downsides**:
  + **Limited Coverage**: Air quality stations are fewer in the UK, so data might not be available for smaller or more rural areas.
  + **Pollen Data is Inconsistent**: Pollen tracking isn’t as robust as other services, and it might not be available for all regions.
  + **Requires Personal Station**: To get more detailed real-time data, users may need to set up their own Air Quality Egg station, which can be inconvenient.

## 5. Pollen Count UK (UK Pollen Count)

* **Website**: Unfortunately, this site doesn’t exist as previously mentioned, and I’m glad you flagged that!

**Alternative to Consider**:

* **Met Office Pollen Count**
  + **Website**: [www.metoffice.gov.uk](https://www.metoffice.gov.uk)
  + **Features**: Offers pollen forecasts and advice across the UK, including tree, grass, and weed pollen.
  + **Downsides**:
    - **Basic UV and Air Quality Data**: It focuses more on the pollen forecast and general weather, not as much on detailed air quality or UV levels.
    - **Generalized Forecast**: The pollen data can sometimes be more generalized, so if you’re in a more localized area, it might not be as specific.
    - **No Dedicated Mobile App**: Although the website is mobile-friendly, there is no standalone app.

# Risks

## 1. Unauthorized Access to Sensitive Data

* **Risk**: Unauthorized users accessing confidential student or business data due to weak authentication mechanisms or role mismanagement.
* **Mitigation**:
* Implement robust role-based access control (RBAC) to ensure users only access data necessary for their role.
* Use multi-factor authentication (MFA) to strengthen user account security.
* Encrypt sensitive data both in transit (using HTTPS) and at rest (AES-256 encryption).

## 2. Weak Passwords or Compromised Accounts

* **Risk**: Users creating weak passwords or reusing passwords from other platforms, increasing susceptibility to brute-force attacks.
* **Mitigation**:
* Enforce strong password requirements (e.g., 12 characters, mix of cases, numbers, special characters).
* Offer passphrase options for usability without compromising security.
* Integrate account lockout policies and rate-limiting for failed login attempts.
* Regularly educate users on safe password practices.

## 3. Data Breaches or Leaks

* **Risk**: Breaches exposing sensitive student and business data due to vulnerabilities in the system or insider threats.
* **Mitigation**:
* Conduct regular penetration testing and security audits to identify and patch vulnerabilities.
* Log and monitor access to sensitive data to detect unusual behaviour.
* Follow a "zero-trust" model, ensuring even internal users have only the necessary access.

## 4. Phishing or Social Engineering Attacks

* **Risk**: Users or administrators falling victim to phishing attempts, leading to credential compromise.
* **Mitigation**:
* Conduct training programs to educate users on recognizing phishing attempts.
* Use email filtering tools to detect and block phishing emails.
* Display last login information to users to identify potential unauthorized access.

## 5. System Downtime or Denial of Service (DoS) Attacks

* **Risk**: A DoS attack could disrupt the service, hindering access to the system.
* **Mitigation**:
* Employ load balancers and distributed denial-of-service (DDoS) protection tools.
* Set up redundant systems to ensure availability during potential downtime.
* Monitor traffic patterns and block IPs showing suspicious activity.

# Decomposition

### Diagram

## Description

# User Acceptance Criteria

# Functional And Non-Functional Requirements

## Functional Requirements

### Definition of a Functional Requirement

A **functional requirement** defines a specific behaviour or functionality that a system or component must perform. It describes what the system should do, such as processing data, responding to user inputs, or interacting with other systems.

### 1.Registration

The core registration system for the product.

#### 1.1 What Details Will be used to sign up

* First Name
* Last Name
* Email
* Password
* Confirm Password
* User Role (drop down)

#### 1.2 Password Requirements

* 12 Characters
* Mixture of upper and Lower-case Letters
* At least one number
* At least one special character

OR

* A Passphrase consisting of three or more unrelated words that are not easily definable or relatable to you as a person from a glance.

#### 1.4 Login

What Details will be used to log in

* Username/Email
* Password

## Non-Functional Requirements

### 2.1 Definition of a Non-Functional Requirement

A **non-functional requirement** specifies criteria that define how a system performs its functions, such as performance, security, reliability, scalability, and usability. It focuses on the quality attributes of the system rather than specific behaviours.

### 

### 2.2 Efficient Loading Times

The system will ensure efficient loading times by optimizing performance to guarantee quick and responsive user interactions. Pages and data will load within three seconds or less, even under heavy usage. Techniques like data caching, efficient database queries, and content delivery networks (CDNs) will be employed to minimize latency. The system will also utilize asynchronous data loading where appropriate, enabling a smooth user experience without delays, especially when dealing with large datasets.

### 2.3 Secure Password Storage

Passwords will be securely stored using a combination of industry-standard techniques. They will be hashed with a secure, one-way algorithm like **bcrypt** (preferred) or **SHA-256**, ensuring resistance to brute-force and rainbow table attacks. Each password will be salted with a unique, cryptographically random salt, and may also be peppered with a secret value to further enhance security. The system will never store plain-text passwords, only the hashed values along with their salts. During authentication, the provided password will be hashed and compared to the stored hash. Additionally, protections like rate-limiting, account lockouts, CAPTCHA, and multi-factor authentication (MFA) will be in place to defend against common attacks.

### 2.4 Secure Data Storage

The system must follow a zero-trust security model, ensuring that access to data is strictly controlled and based on the principle of least privilege. This approach will limit data visibility, with users being granted access only to the data necessary for their role and tasks. All access permissions should be continuously validated, ensuring that only authorized users and systems can interact with sensitive data. Data should be encrypted both in transit and at rest, and no user or system should be trusted by default.

# Key Performance Indicators (KPIs)

## What Are KPIs?

**KPIs (Key Performance Indicators)** are measurable values that indicate how effectively an individual, team, or organization is achieving specific objectives. They help track progress, assess performance, and guide decision-making to meet goals.