**Risk Assessment:**

The project uses geographical data to show asset locations on a map. Potential hazards which are related to creating a web-based asset management interface for the City of Bradford Metropolitan Council are identified in this risk assessment. By addressing these risks, we can ensure that responsible and secure features and methods are implemented into the system.

**Risks:**

|  |  |  |  |
| --- | --- | --- | --- |
| Legal Issues | Social Issues | Ethical Issues | Professional Issues |
| Data Privacy and Protection | Accessibility | Data Ownership | System Downtime and Dependency |
| Data security Measures | Transparency and Fairness | Fairness in Asset categorisation | Cybersecurity |
| Liability and Data Accuracy | User adoption and engagement | Quality Assurance | User Authentication & Data security |

**Data Privacy and Protection:**

The system will keep and process sensitive and personal data. If the data is handled unlawfully, it would violate the UK Data Protection Act 2018. The impact of this would result in penalties and loss of trust. To avoid breach of personal data, ensure to anonymise sensitive data where possible. Encrypt sensitive data and provide a clear consent procedures on how a user’s data is being used.

**Data security measure:**

Implementing robust security measures, such as access controls and regular backups, is essential to protect users’ information from unauthorised access. Compliance with relevant data protection laws and regulation should be ensured. Access controls restrict data access to authorised personnel only. Frequent backups decrease the chance of data loss from cyberattacks or system breakdowns.

**Liability and Data Accuracy:**

Two important concerns while developing the web interface are liability and data accuracy. Inaccurate data on the map may cause users to make poor decisions, misuse the system, and compromise its reliability. For example, displaying an asset’s location incorrectly could ultimately provide the user with inaccurate information and result in inefficiencies or even community safety risks. You may be responsible for any errors especially if the data is utilised for important business processes or decision-making. Therefore, it is important that the data is updated regularly, verified and cross-checked for accuracy before displaying it on the web interface.

**Accessibility:**

The application should be designed so that it is accessible to all users, considering any physical abilities. To do this the application must comply with the accessibility standards and guidelines such as the WCAG (Web Content Accessibility Guidelines). To ensure that all users, regardless of ability, have an inclusive experience, features like keyboard navigation, screen reader compatibility and alternate text for images. The system should also accommodate assistive technologies like speech recognition software’s.

**Transparency and Fairness:**

Fairness and transparency are important for gaining the user’s trust. User’s must be given the opportunity to provide their consent and be fully informed about how their personal data is being gathered, utilised and stored by the system. To prevent any prejudice, users should also be informed about the classification and representation of the assets and associated data. Users should have access to their data and should be able to adjust. The platform should respect their right to control their own data.

**User Adoption and Engagement:**

The system’s success depends on the user involvement and how easy it is to adopt the web interface. If it is difficult to use many consumers could hesitate to use it. The system needs to be simple to use and clear to encourage adoption. This would increase engagement, especially if it delivers relevant features and offers useful directions. Maintaining user engagement can also be achieved by offering continuing support, gathering user input and issuing frequent updates in response to this input.

**Data Ownership:**  
As mentioned before, users should have control over their own data and they should be informed about how it is being used, stored and shared within the system. Prior consent should be obtained to collect this data before it is collected- usually via a popup. In accordance with their ownership rights, people or organisations must be able to view, update or remove their data without any interference. To avoid misuse, the system should include explicit data ownership policies and procedures that outline how data will be shared, kept or used.

**Fairness in Asset Categorisation:**

When creating the system, assets must be categorised honestly to prevent any unfair disadvantage or misinterpretation of any organisation. It ensures that every asset is handled properly. To avoid any discrimination being unintentionally included into the system, each algorithm used to categorise assets must undergo routine audits. User’s must also have the confidence that all categories are well-supported and justified and no group is favoured over another. By making sure that everyone feels treated fairly and without bias, transparent categorisation enforces user’s trust.

**Quality Assurance:**

Since inaccurate data can result in poor decision-making, it is imperative that the data presented is accurate and current. Before the system is used by the user, possible faults in its functioning, design and data can be found and fixed. This can be done by carrying out routine audits, checking for errors and confirming that every feature functions as planned. The system must be tested under real-world circumstances to fulfil the needs of a wide range of users. Furthermore, to increase the system’s dependability, you should make sure that any updates do not unintentionally harm the quality of the interface.

**System Downtime and Dependency:**

This describes a faulty system due to server failures or technological difficulties. System dependency and downtime can cause serious problems since extended outages can result in service interruptions and monetary losses. Implementing a strong infrastructure and monitoring tools is necessary to mitigate these risks and guarantee system reliability and reduces downtime. Reducing the impact of dependency can be achieved by providing backup solutions during outages.

**Cybersecurity:**

Cybersecurity for the web interface guarantees confidentiality and integrity of data held in the system. Maintaining strong cybersecurity standards, is essential to guard against breaches, hacking attempts as the web interface will store sensitive data. Inadequate cybersecurity safeguards can result in the user’s personal data being accessed without authorisation and ultimately resulting in legal issues. Encryption, firewalls and frequent security audits are an important part of cybersecurity. Reducing the vulnerabilities requires keeping the system updated with recent security updates.

**User Authentication:**

A strong user authentication method should be implemented, such as multi-factor authentication, to help prevent unauthorised access to the system and safeguard sensitive data from malicious actors like cyber attackers and data breaches within the application. Strong authentication and data security procedures are put in place to safeguard user information, lower the possibility of breaches and uphold the system’s credibility.