**The Design Proposal Document – School Learning Management System**

**Introduction**

This document covers the development of a secured learning management system for schools (Se-LMS). The Se-LMS allows teachers, students and parents to view students’ assignments and grades securely. Se-LMS have been promoted in the UK over the last decade (Ofsted, 2013) while the Department for Education (DfE) require schools to provide high-quality remote education (DfE, 2024).

**System requirements and specification**

Users will log-in to the system using a secure password. The system security can be turned on or off. Users will perform role appropriate Create, Read, Update, and Delate (CRUD) functions. Roles will be managed by the administrator. Appropriate legal frameworks, including GDPR will be observed, such as data minimisation. Minimum system requirements are shown in Appendix 2.

**Functional requirements of the application**

The Se-LMS will incorporate several components outlined by Patel, Gadhavi & Patel (2013):

* Administrators will be able to add new courses, update existing courses, assign teachers to courses, register, view, and enrol students or manage their profile.
* Teachers will be able to upload content, view assignments, and provide feedback and grades.
* Students will be able to view content, see their own grades, and submit work.
* Users will require secure account log-ins.

**Legal requirements**

GDPR regulations regarding its processing of user data will be adhered to:

‘Consent for the processing of the users’ personal information must be obtained from students aged 13 and over, while consent from parents must be obtained for those under 13’ (Calder, 2018).

To comply with article 5 of the GDPR (Calder, 2018), the following steps will be taken:

* Users’ personal data will not be shared with third parties
* Users will be informed on how their data will be used.
* Personal data will only be used to inform teachers of who their students are and how they are progressing.
* Only relevant student data will be collected to ensure the functionality of the Se-LMS: first and last names, age, assigned teacher, and assignment marks; and for teachers: first and last names, subject speciality.
* The above data will be updated, when relevant, by the administrator.
* When a student leaves the school, their data will be deleted manually by the administrator, on 1st September.
* Security procedures will be followed to secure data processing, as seen below.

**Security Requirements**

Secure authentication will be achieved by implementing role permissions. For example, only admin users will be able to register new students (MITRE, 2017). In addition, user passwords are hashed before being compared to the record of hashed user passwords (Spraul, 2015). Users’ attempts at inputting their passwords will also be restricted to protect against Brute Force Attacks (Spraul 2015) and user credentials will be confirmed using Multi Factor Authentication (Spraul 2015). Event monitoring will be enforced by logging attempts made by users to log-in as an administrator (Kellezi et al., 2021). SQL injection attacks will be protected against by ensuring that user input is sanitised and never used directly for database queries (Galluccio, et al, 2020). Denial of service attacks will be mitigated against by ensuring that regular expressions are not exploited, with correct sanitisation of user input implemented and input evaluation times handled appropriately (Larson, 2018).