**NUA**

Student Portal

Joshua Leivers | 6033

28275

Contents

[1 Analysis 2](#_Toc14424574)

[1.1 Introduction 2](#_Toc14424575)

[1.2 Existing Systems 2](#_Toc14424576)

[1.2.1 Moodle 2](#_Toc14424577)

[1.2.2 SIMS 3](#_Toc14424578)

[1.3 End Users 4](#_Toc14424579)

[1.4 Objectives 4](#_Toc14424580)

[1.5 Constraints and Limitations 6](#_Toc14424581)

[1.6 Proposed Solution 6](#_Toc14424582)

[1.7 Evidence of Analysis 6](#_Toc14424583)

[1.7.1 Interviews 6](#_Toc14424584)

[1.7.2 Questionnaires 7](#_Toc14424585)

[1.7.3 Online Research 9](#_Toc14424586)

# 1 Analysis

## 1.1 Introduction

A student portal is an online gateway and system for providing students of a school, college or university with access to important academic information, resources and statistics (such as grades, attendance, announcements, etc.), software for download and use, links to other academic websites, and useful webpages.

Such a portal would usually use an existing login system/database, as well as linking in with the registration/academic records of the school, but this may conflict with GDPR or the Data Protection Act.

The system behind a student portal would use a database of connected tables, a web application and a script/program of some kind to either link into existing academic databases/information, or to export information from the existing records and import them into the student portal’s database.

## 1.2 Existing Systems

NUAST currently uses Moodle, SIMS, Office 365 and a website. SIMS and Office 365, as well as the school network/computers, are connected to shared resources with the Nova Education Trust, which the academy is a part of, meaning the trust’s policies apply.

Except the website, which only provides generic information and forms to fill in, and does not require logins for anything, all of the school’s systems share a login system. This login system is Microsoft’s Active Directory, and while it is technically possible for my project to use this system for users to log in, the school/trust’s policies do not allow this.

### 1.2.1 Moodle

Moodle allows teachers to set up “courses” which they can add students to, where the teachers can upload links and files for students in the course to download. This covers part of what a student portal should do, and so my project should focus more on the other aspects of it.



Figure 1.2.1.1 Moodle Course Overview

Moodle also allows teachers to add announcements, news and events, however the implementation of this is not effective, as each individual course has an announcements section and users are not notified in any way if there are new announcements.



Figure 1.2.1.2 Moodle Course Example

### 1.2.2 SIMS

SIMS is the registration system used by the academy, which records student attendance, detentions and academic information – including student timetables. For anything relating to these statistics and information, my project will probably need to link into or work with SIMS in some way. Staff mainly use PARS for interacting with SIMS, but SIMS is the system that controls everything and that my project would need to interact with.



Figure 1.2.2.1 SIMS Interface

SIMS is primarily an information management system, based on a large database containing student information. My project ideally would link with this database, rather than interact with SIMS – as this would easily allow my system to access up-to-date info such as a student’s attendance without taxing resources. However, SIMS’ database operation is subject to change between updates, and is deliberately not easily accessible. Instead, SIMS is able to automatically generate reports, so I may be able to either schedule reports to be exported, which can then be accessed by my system, or set up a script that does this instead.



Figure 1.2.2.2 SIMS Report Options

Linking into SIMS would require high standards of data protection and cyber security, as confidential information is stored in SIMS, and my system should be secure and only allow users access to information they are allowed to access.

The school/trust is currently planning on changing to a different information management system next year, which likely will mean a different database structure and report system. This would require certain parts of my project to be changed if the school implements it in the future, specifically anything that requires access to the database or SIMS reports, but the existing features would almost certainly be available within the new system, and would only need small query changes and/or new report scheduling (as well as report handling).

### 1.2.3 Website

NUAST’s website is mainly used for sharing general information with the public and with parents. This means that no information is about any specific student, so most of the information it provides would be different to what my project would provide access to.

In terms of tools, the website only provides forms for anyone to fill in. This includes a contact form and a form for people to send any concerns they have to staff. This form does part of what I wish for my project to do, however it is potentially unsecure, as it uses email to send form responses, and the form is not widely known to students.



There are also forms to fill in to give general feedback on different topics such as homework, however as these use SurveyMonkey, and no verification of identity, anyone can submit as many of the questionnaires as they want, skewing results and/or rendering submissions useless.



## 1.3 End Users

There are varying end users for this project. The main end user would be the students, who the majority of systems within the project would be aimed towards. However, there would be other end users, these being teachers and other school and trust staff. These users would be able to access different tools and parts of the application depending on their roles.

For example, a computer science teacher who is also part of the safeguarding team would be able to interact with computer science students within tools, and would also be able to access tools available to the safeguarding team (e.g. see safeguarding reports), but would not be able to view their own attendance, as it would not be recorded.

Currently, students do not have a way to access their academic information without asking teachers to manually find it, or from reports, which are not released often. They also do not have a way to make suggestions or report issues securely, nor do they have a way to easily see what homework has been set, information about it, or easily receive or set reminders about it.

Staff do not have an easy method to send a message to different groups of people within the school or to receive reports and suggestions.

Teachers do not have a method to set homework for their students online for them to view, or to set reminders of homework for them.

## 1.4 Objectives

|  |  |  |
| --- | --- | --- |
| No. | Objective | Performance Criteria |
| 1 | Create a secure login system to access the student portal | This must use salting and hashing, with each user having their own random salt, to login. Every time a password is entered, it must be salted and hashed using a secure hashing algorithm. Passwords must not be stored unsalted and unhashed anywhere. Each user’s salt must be randomly generated upon the creation of the account and be stored within the login information table. This salt must be unique, with no other user having the same salt, and long enough to be so.  No tools or information should be accessible unless the user is logged in. Logins should persist unless the user logs out, is logged out, their browser user agent changes, changes occur to the account that require the user to be reverified (e.g. password changes), or the account is disabled, deleted or suspended.  Any previous or active login should be recorded, including the time of login, time of logout, IP address and user agent. |
| 2 | Data protection legislation and policies should be adhered to and data protection should be done to the highest reasonable standards | No user should be able to access data that they are not authorised to access. Users should only be able to access their own information, and if they are a staff member, only allowed to access information for students and other staff where it is appropriate, legal, and makes sense. |
| 3 | Students should be able to view their own attendance information, timetables and grades from SIMS | This information must be obtained from SIMS, and kept reasonably up to date, with information updated at least every 24 hours, except under certain conditions, such as technical issues, and if the students are on a break from school. |
| 4. | Users should be able to receive notifications through the web app | These notifications should appear within the web app, and be sent in push notifications where possible (such as through Google Chrome). |
| 5. | Users should be able to send notifications to other users through the web app where appropriate | Users must only be able to send notifications to other users appropriate to their relationship. For example, a teacher to the classes and students they teach, a student council head of year to students in their year, a head of department to teachers and students within their department, and the head teacher to every student and member of staff. Sent notifications, their recipients, and when they were sent, should be logged. |
| 6. | Every person within the school should have their own account within the web app | Every student, teacher and staff member should have their own account, with the username being the same as their username within other school systems. Each account should have set permissions depending on the user’s role within the school. These accounts should either be created automatically based on information from school systems, or be created upon request, requiring new users to verify their new account via school email. |
| 7. | Users should be able to set their own password | Users must be asked to set a password upon account creation/first login. They must be able to change this password at any time from the web app. No other user should be able to set another user’s password. Technicians/admins should only be able to trigger a password reset, not set a new password. When a new password is set, the information on how it was set should be logged, including login session ID, time, and method. |
| 8. | Users should be able to reset their password if they are unable to get into their account | A password reset should be able to be triggered by a ‘forgot password’ function, and by a technician/admin. Once a reset is triggered, an email should be sent to the user’s school email, including a link. If the user clicks on the link, they should be taken to a page to create a new password. If they do not click the link, their password should remain unchanged. A user should be able to click a different link in the email to mark a reset request as suspicious, and to add a message, which technicians/admins should be able to view and take action on, by either doing something about it if it is a technical issue, or by notifying other appropriate staff members if it is either a safeguarding or punishment issue. Password reset requests should be logged, including the method they were triggered, who by and what session ID (when by technicians), IP address and user agent (when from ‘forgot password’), and whether they were confirmed. |
| 9. | Passwords must be secure | When a user attempts to set/change their password, the new password should be denied if it:   * Does not contain a lowercase letter, uppercase letter, number and special symbol * Matches a dictionary of common/breached passwords (possibly using the haveibeenpwned API) |
| 10. | Users must be asked to reverify their password to access confidential information, change important/security settings, or to access secure tools | Whenever users attempt to access anything that is confidential/sensitive, or to change any important/security settings for the system or for their account, they must be prompted to re-enter their password, and two-factor authentication code if enabled, to be able to access it. If they enter an incorrect password three or more times, they should be forcefully logged out and the incident logged for the user and technicians/admins to see. Otherwise, if they cancel accessing that tool/information, they should be returned to the previous page but not logged out. |
| 11. | Users must be able to enable two-factor authentication on their accounts | This two-factor authentication should use TOTP 2FA, specifically allowing the use of Google Authenticator. Users must be able to enable or disable this within their account settings. |
| 12. | Technicians/admins and leadership staff (e.g. head teacher, head of sixth form) should be able to disable users accounts | In case of an account breach, investigation, or other circumstances, technicians and high-level staff members should be able to disable users accounts, leaving the accounts still there, but not allowing users to log into them. To disable the account, the user doing so must give a reason, which should be shown to the anyone attempting to log into the disabled account. Technicians and high-level staff members should then be able to re-enable disabled accounts.  Whenever account is disabled or re-enabled, the account it is done to, the user that did it, the time, session ID and reason. |
| 13. | Upon account creation, permissions should be set for the new account automatically where possible | The system should be able to identify if the user is a student, teacher or staff member, who they are on SIMS, and from that identify what classes they teach/have, retrieve academic information for the user where applicable, and assign permissions based on their role within the school. A high-level staff member or technician should be able to change, add or remove permissions in case the user should/shouldn’t have permissions but that information isn’t available from SIMS. |
| 14. | Students should be able to report issues and make suggestions using the web app | Students should be able to report different types of issues and make suggestions, being able to select a category, department, etc. and then write a message explaining their issue/suggestion. For example, a student could report a safeguarding issue, in which case safeguarding staff would be able to read it, or suggest new equipment/services to the computer science department, or report maintenance issues.  Students should have the option for these reports and suggestions to be anonymous, in which case the origin of the report/suggestion should not be recorded, with staff receiving it only seeing the message and that the student is anonymous. There should be no way to circumvent this. |
| 15. | Teachers should be able to set homework for students to see using the web app | Teachers should be able to set homework for specific students or classes they have, including the due date and any information about the homework (i.e. what the homework is). They should be able to set reminders about the homework for themselves and for the students it is set for. They should automatically be reminded at the start of the lesson it is due for.  Teachers should also be able to mark set homework as received, late, cancelled, or not handed in. |
| 16. | Students should be able to view homework set for them using the web app | Students should be able to see what homework has been set, when it is due for, what teacher set it, when it was set, who was it set for (which class or group of students) and any extra information about the homework.  Students should also be able to set reminders for themselves about the homework set, add notes about the homework set, and mark whether they have completed it, have started it, or haven’t started it (should be set to haven’t started by default) |

## 1.5 Constraints and Limitations

* Access to student information must comply with data protection legislation (mainly GDPR and Data Protection Act)
* There is no readily available SIMS API and accessing the database directly is not possible due to updates changing its structure
* NUAST/Nova Education Trust’s policies may not allow access to some tools, software and/or information

## 1.6 Proposed Solution

A web app written in Python using Flask that uses an SQL database to store login, security, settings and other information uploaded to the app. This web app would use a secure login system to be able to access any tools or information. In addition to this, scripts and/or scheduled tasks would be set up to export student information from SIMS every 24 hours to the app’s database for students to access. The app would allow students to report issues and make suggestions in different categories (e.g. physics, safeguarding, maintenance).

### 1.6.1 Languages

As the majority of my project will be focused on the web application, the web app will have to be programmed in one of the five language options for the NEA. Out of these, Python and Java are very popular for web development.

Comparing the two, and from research online, I have found that Python is much more modern, and is often favoured due to its high speed delivery and low overheads. There is a very active developer community based around Python web development, whereas Java web development tends to be based around enterprises, so it would likely be much easier to find information and documentation for Python-based web development. This should cut time down for programming greatly.

On top of the web app, there also may need to be scripts run for exporting SIMS information to my database, and Python would allow this to be done very lightweight.

NUAST’s computers also tend to have issues running some parts of Java, but have no issues running Python.

Together with the web app and scripting, there would also need to be web pages to display, which would need to be written in HTML, however for styling, I intend to use the CSS from NUAST’s website to keep styling consistent, perhaps with some minor changes to allow dark and light modes.

In conclusion, Python would likely be the best choice of programming language for the web application and scripting, along with HTML for web pages, and some minor use of CSS for alternative styling.

### 1.6.2 Frameworks

There are two very popular frameworks for Python web development: Flask and Django. Django is has been around much longer and is much more popular than Flask, however Flask has massively less overhead and tends to be much faster. In exchange for the overhead, Django also provides a lot more functionality, however much of it would not be useful for my project.

In conclusion, the best web framework for Python to use for my project would be Flask.

### 1.6.3 Developer Environment

As the entirety of my project will be based around Python, with side elements of HTML and CSS, using a full IDE would only complicate development, and so I intend to use a text editor, then run files separately.

For a text editor, I intend to use Atom, as it also provides some IDE functionality that may be useful for development.

To test my project, I will use Google Chrome, Mozilla Firefox, Internet Explorer, and Microsoft Edge. Together, these browsers take 72.76% of the overall usage share of web browsers, 90% of the desktop web browser usage share, and 60.87% of the mobile market share.

Another browser, Safari, is very popular within the Apple ecosystem, and has an overall usage share of 15.15%, desktop usage share of 3.32%, and mobile usage share of 20.12%, and would be useful to include in my testing. However, I do not have access to any device which can use Safari, and so I am unable to test this actively. A lot of what works within most other browsers, but especially Chrome (as it uses Blink, a fork of WebKit which is Safari’s engine) should work within Safari.

## 1.7 Evidence of Analysis

### 1.7.1 Interviews

#### 1.7.1.1 IT Technician

**Q.** What does the school use for a login system?

**A.** Microsoft’s Active Directory

**Q.** Would it be possible to link my student portal with the school’s login system?

**A.** No. Keep everything separate from the school system.

**Q.** When is the school changing away from SIMS?

**A.** Next year

**Q.** Would it be possible to set up a system on the school network where reports from SIMS are scheduled to be exported every 24 hours, converted to CSV using CommandReporter, then uploads the CSV file to my database?

**A.** <ASK WHEN AVAILABLE>

#### 1.7.1.2 Head of Computer Science

**Q.** Does the school have access to CommandReporter for SIMS?

**A.** Yes

**Q.** Can SIMS schedule reports for teachers?

**A.** Yes. Using PARS, teachers can even have reports automatically emailed to them on a schedule.

### 1.7.2 Questionnaires

#### 1.7.2.1 Students’ Opinions on Usefulness











### 1.7.3 Online Research

#### 1.7.3.1 SIMS

From doing research online, I found that SIMS’ database structure tends to change between updates, and so hooking directly into the database in my app would likely only work for a short time, before a new update changes the database structure and breaks any queries within the changed tables.[[1]](#footnote-1)

In general, the suggested way to access information from SIMS is to export reports (this can be scheduled using Task Scheduler), have them converted to CSV files by CommandReporter, then import them into the system that the user wants the data in.[[2]](#footnote-2)

#### 1.7.3.2 Website

The website does not provide many tools, mainly providing general public information about NUAST, however there are forms that can be filled out. One of these is a form for reporting issues, optionally anonymously. However, this form sends the results via email[[3]](#footnote-3), which can be insecure during transit – especially if unencrypted – and upon receipt.[[4]](#footnote-4)

# 2 Design

My project will be split into three components that interact with each other. These components will be the database, report scripts and web application.

The report scripts will gather information from reports exported by SIMS and upload it to the database.

The web application will contain a secure login system and allow users to access tools and information appropriate to their role within NUAST.

## 2.1 Database

The database will store multiple tables. These tables will contain login and personal information, and any information that should be actively available within the web application. The database will use MySQL.

The database can be created using the following query:

**CREATE DATABASE nea**

### 2.1.1 Users

The users table will store any information required to identify individual users, including their username, salted and hashed password, permissions, forename and surname. Their username will be used as the primary key, as it will always be unique.

#### 2.1.1.1 Table Structure

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Field Name | username | password | forename | surname | permissions |
| Type | VARCHAR | CHAR | VARCHAR | VARCHAR | VARCHAR |
| Size | 34 | 60 | 102 | 102 | 102 |

#### 2.1.1.2 Table Creation

The Users table can be created using the following query:

**CREATE TABLE IF NOT EXISTS users ( username VARCHAR(20) NOT NULL, password CHAR(60), forename VARCHAR(64), surname VARCHAR(64), permissions VARCHAR(32), PRIMARY KEY ( username ) )**

### 2.1.2 Sessions

The sessions table will store the information about any active or recent login sessions, including their unique ID, username, when the session began, when it ended, the IP address and user agent. The session ID will be the primary key

#### 2.1.2.1 Table Structure

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Field Name | sessionid | username | start | end | ip | useragent |
| Type | CHAR | VARCHAR | DATETIME | DATETIME | INT UNSIGNED | VARCHAR |
| Size | 64 | 34 | 8 | 8 | 4 | 102 |

102 bytes long due to 100 chars max + 2 bytes of field data

Flask Bcrypt, 72 chars password max unless workaround

User agent, use from user\_agents import parse, parse(useragent), store parsed form

1. <http://www.edugeek.net/forums/mis-systems/63879-sims-database-structure.html> [↑](#footnote-ref-1)
2. <https://blogleedrury.files.wordpress.com/2019/03/command-reporter-user-guide.pdf> [↑](#footnote-ref-2)
3. <http://nuast.org.uk/page.php?p=pupil> [↑](#footnote-ref-3)
4. <https://support.google.com/transparencyreport/answer/7381230?hl=en> [↑](#footnote-ref-4)