Security

Security is a key aspect in creating any type of system. Here we will discuss how we intend to make sure our system is secure, and our data safe.

Sensitive Data

The system we are creating will host various types of data from usernames, to passwords, food, ID numbers and more. It was expressed during our meeting with Veronika that student ID numbers are considered to be extremely sensitive data, and therefore must be treated with great care. It is her wish for us to figure out a way in which even the people with access to the system do not know the student's personal ID number.

Passwords and personal information (of both staff, and users) are also data that we will consider to be sensitive, and will treat with great care. This type of information must be handled as such, in order to keep not only the system secure, but also the users.

How we will protect this data

Student ID's – Keeping student ID's private is something that Veronika has deemed a top priority, and we will treat this as such. One likely solution to this is to use hashing on student ID numbers. In short using this method, students will only have to provide their ID number one time. After this initial process, the students ID number will be uniquely mapped to a new key which they themselves as well as the database administrators, staff, and system will use to identify the student.

Passwords & Personal Information – There are a number of methods to secure this data, but to name just a few we will be using HTTPS on the website/system which means data such as passwords will be encrypted, therefore what is sent to the server is not just plain text and therefore cannot be simply seen/copied.

Furthermore we will take precautions such as;

- o Encrypting even our backups

- o Ensuring privileges are assigned to only those who need them

- o Installing security patches frequently and on time

- o Removing unused modules, applications & services.