# Role-Based Security System

**Created by Mark Tickner**

The site is based on a role-based security system, meaning that users can have different levels of access and permission to view specific pages that are relevant to them on the site. For the eSupervision system, the types of user required are students, staff (supervisors and second markers) and authorised staff. Students have access only to student specific pages, staff have access to a subset of staff specific pages and authorised staff have access to all of the staff pages.

This has been implemented at database level firstly by storing staff and student records in separate tables. The decision to store them separately was made as the implementation of the tables is required only for this project, as in the live system the user data would be sourced from the university’s MIS (Management Information System). The structure of these tables is very similar.

When the user attempts to log in, the provided credentials are cross-referenced in both of these tables to determine if a match is found; if no match is found, login is declined and an error message is shown. A check is also made against the ‘active’ column in the table to determine if the user is a currently active student or staff; if the user is not active, login is declined and an error message is shown. If a match is found, the details of the user, type and authorisation (if staff) is stored in a server session and log is accepted.

The ‘type’ and ‘authorised’ variables in the session are the key part of the role-based security system. They are both checked on every page the user visits to ensure that access is allowed, and if not the user is redirected back to their appropriate dashboard. As this is all on the server-side, it is a secure form of access control. It also means that a member or staff can be changed between authorised and unauthorised just by setting the appropriate field in the database.