Group declaration of Academic Honesty

Subject Code/Name:	INFO30005 – Web Information Technologies
Assignment Title:	Part B – Project Plan and Application Design
Tutorial Day/Time:	Friday 3 PM
Tutor/Instructor Name:	Mitchell Harrop
Submitted Date/Time:	3:30 PM
Group number/name:	Double D

Declaration

We declare that this assignment is our group's own work and does not involve plagiarism or collusion. We also declare that the material contained in this assignment has not previously been submitted for assessment in any other formal course of study. Furthermore we declare that (place a cross in each box):

- □ we did not cut-and-paste information from others without appropriate use of quotation marks and direct reference to their work;
- □ we did not re-word the ideas of others without proper and clear acknowledgement;
- □ we did not write ideas or suggestions that originated from other students and claim these as our own;
- □ we did not include words from other students' work unless this was explicitly permitted in the description of this assignment.
- □ we have not made any other violations of the University's Plagiarism and Collusion policy (see next page).

We understand that any violation of the above will result in a possible:

- ○ ZERO mark for this assignment, and/or
- ○ ZERO mark for the subject, and
- ○ our names will be recorded on the DIS Plagiarism database and will be forwarded to the Faculty of Science to be recorded on the Faculty's Plagiarism Database. This could lead to termination of our places at this university.

For assessment purposes, we give the assessor of this assignment the permission to: reproduce this assignment and provide a copy to another member of staff; and take steps to authenticate the assignment, including communicating a copy of this assignment to a checking service (which may retain a copy of the assignment on its database for future plagiarism checking).

	ID	Full name	Signature	Date	Contribution (total must sum to 100%)
1	583334	Daniel Masters	Daniel Masters	01/04/2014	33.3%
2	358064	Daniel Esposito	Daniel Esposito	01/04/2014	33.3%
3	582823	Hoang Dieu Anh Nguyen	Hoang Nguyen	01/04/2014	33.3%

Note: For electronic submissions the signatures may be typed. Also, unless otherwise indicated, it will be assumed that all group members made an equal contribution to the overall effort. If a dispute arises, the matter should be reported to the lecturer-in-charge for consideration.

Project Plan and Application Design

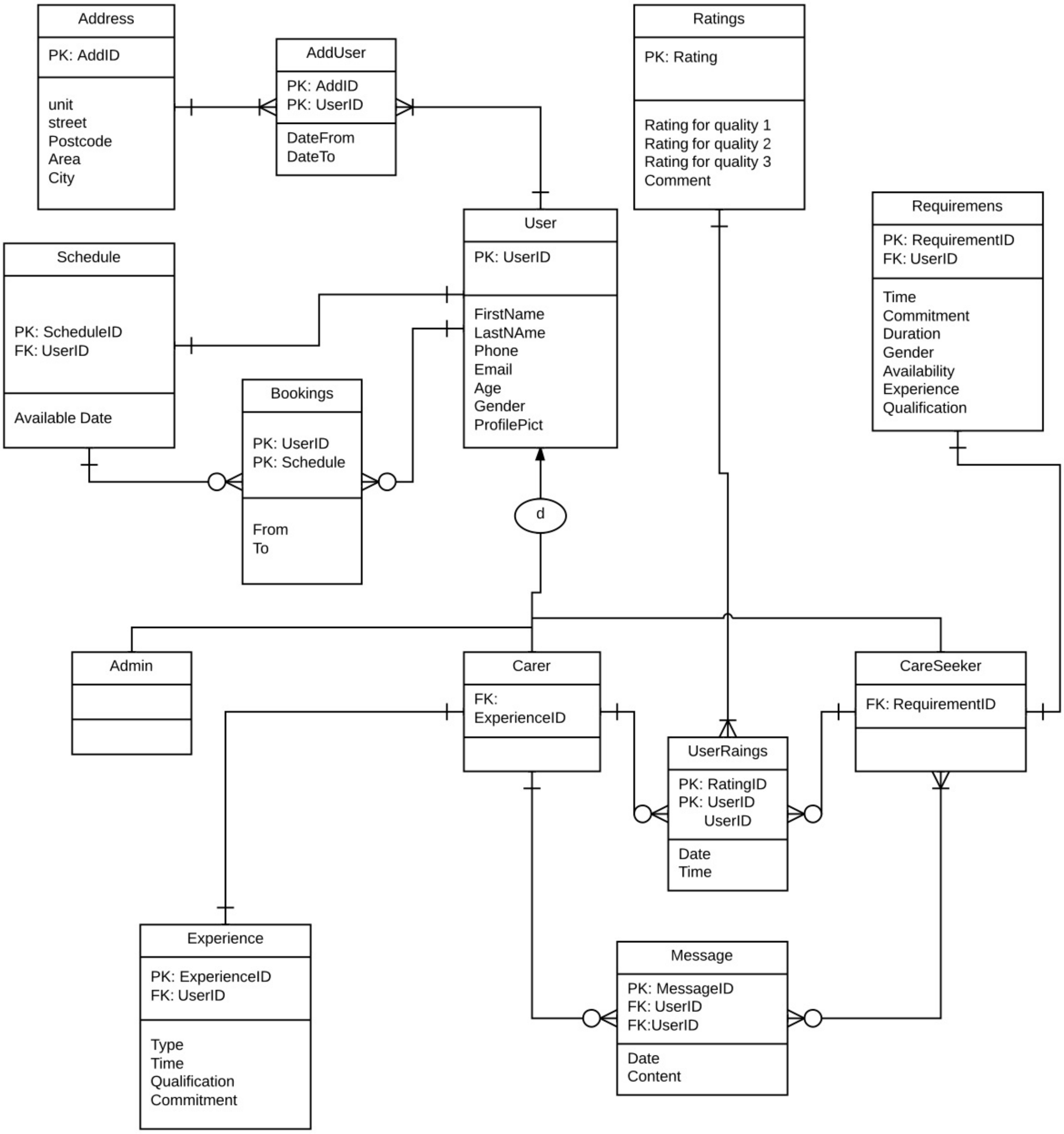
WEB INFORMATION TECHNOLOGIES

Daniel Masters – 583334
Daniel Esposito – 358064
Hoang Nguyen – 582823

Friday 3 PM

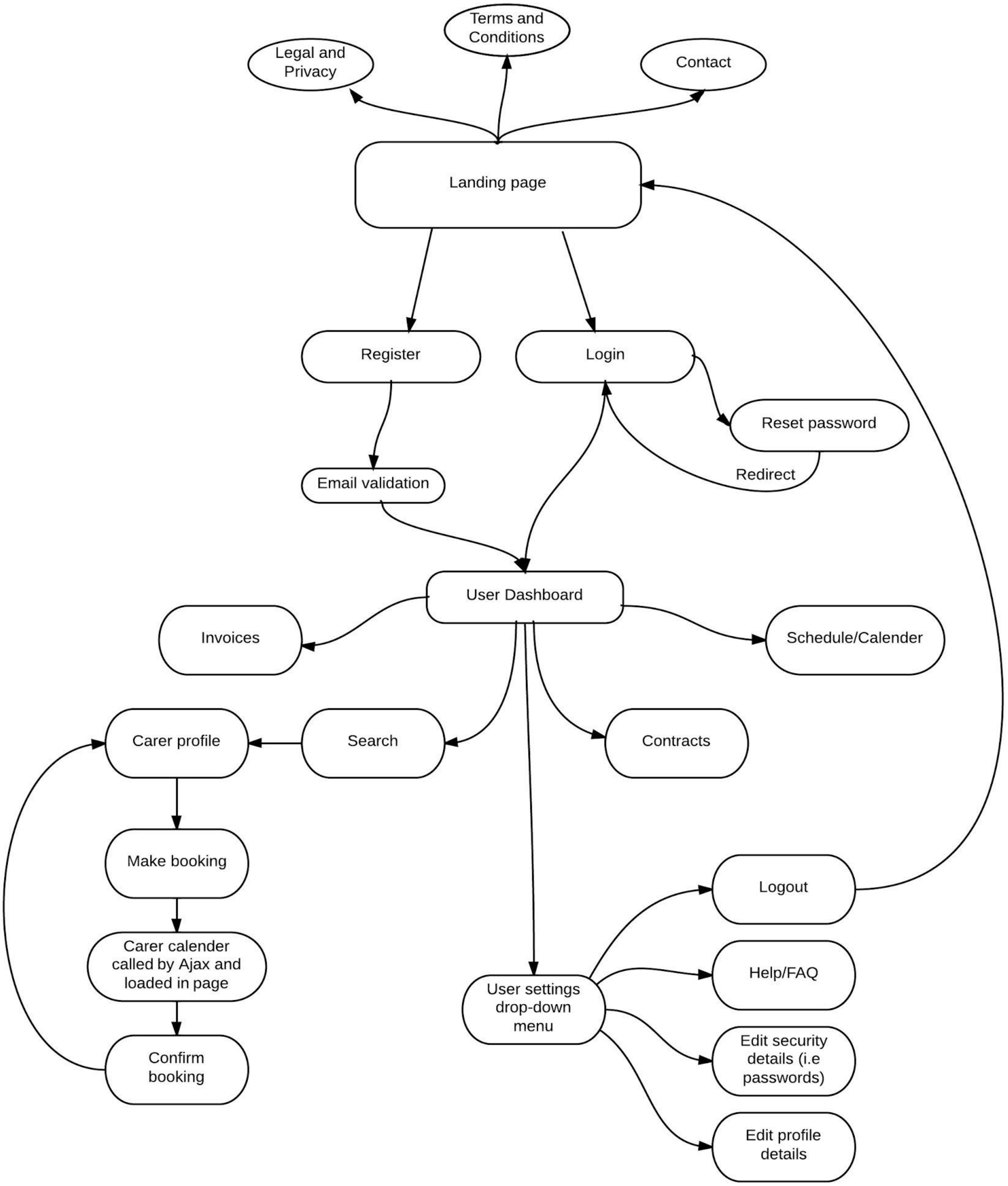
Model

Data Design



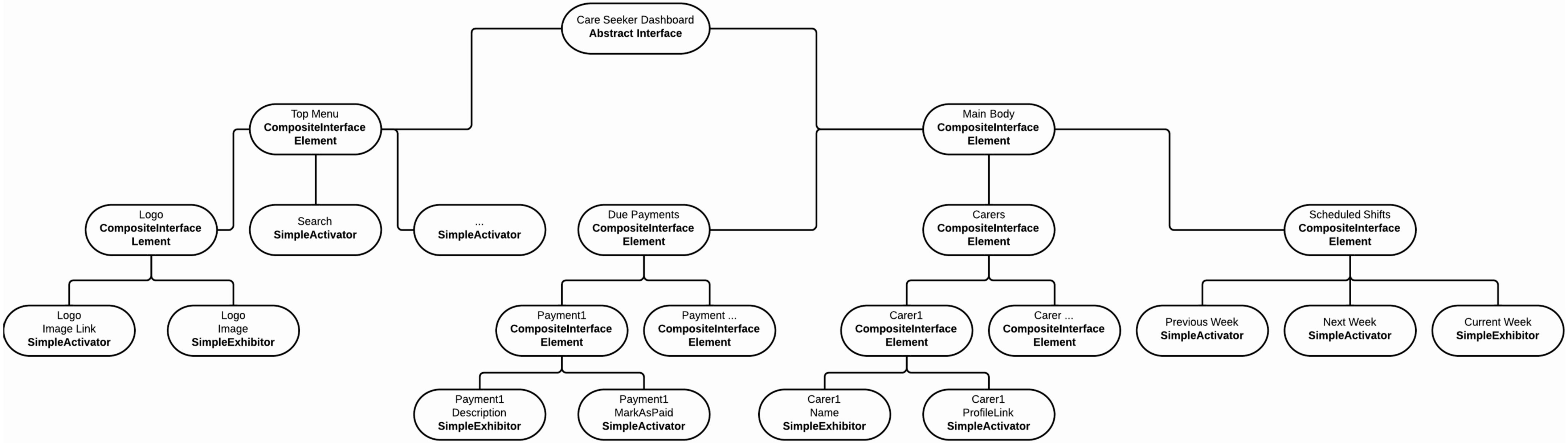
Navigation Design

The possibility that handicapped users may be using CareSeek introduces several design considerations that must be prioritised. This can be addressed by ensuring site navigation is simple, page presentation is compatible with various accessibility devices (e.g. screen readers), and HTML code is well-formed and contains alt tags.

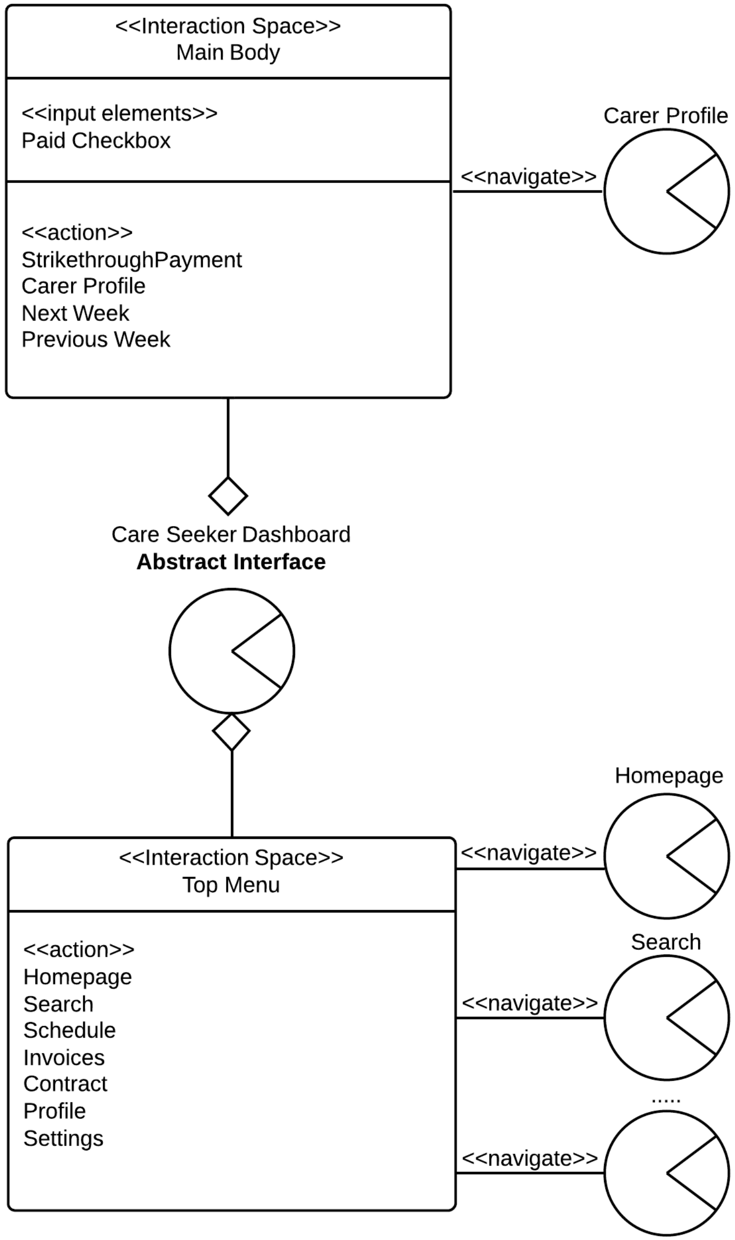


Presentation Design

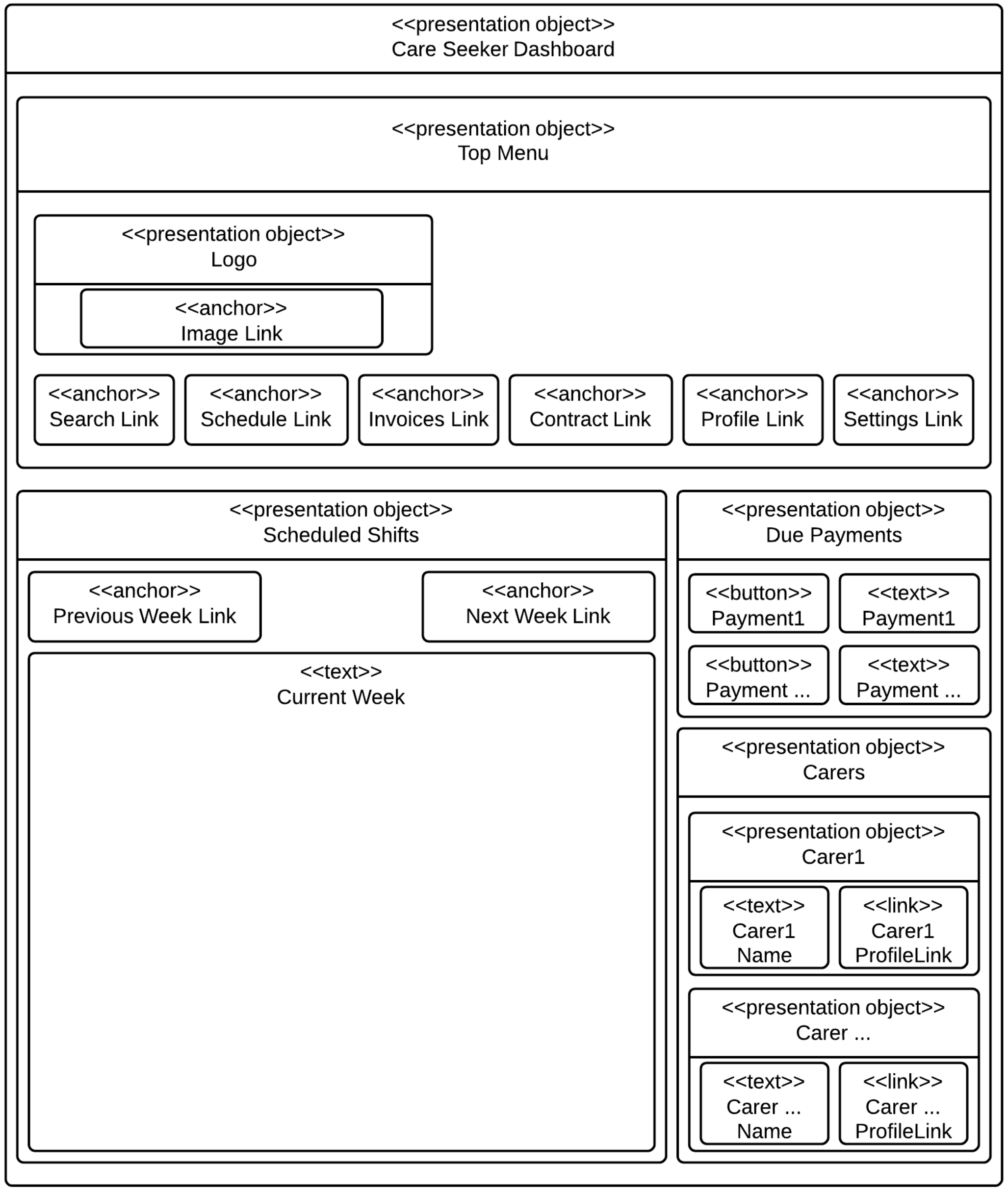
Abstract Widgets Design



Interaction Space Design



Concrete Presentation Design



Technology and Infrastructure

Back-End Language

We selected Python as our back-end language, as it has numerous advantages.

The Python syntax is readable and clear. It uses dynamic typing, late binding and a cycle-detecting garbage collector for memory management. Python’s powerful library motivates programmers to follow the "don't repeat yourself" (DRY) principle. Programmers can also share functionality between different programs just by dividing them into different modules and reusing them in other programs.

Front-End Languages

HTML5

HTML5 is supported by many browsers such as Chrome, Firefox, Safari, Opera and even many mobile browsers. The aim for this project is to create an interactive web application, which can be achieved using HTML5.

CSS

Cascading Style Sheets (CSS) was selected because it enables separation of content and style, which results in a reduction of HTML code; this means webpages will load faster. It also means creating a responsive web application will be simpler. CSS also offers more stylistic possibilities when compared with HTML5, which means we have more visual options at our disposal.

Bootstrap

Bootstrap is a CSS framework that provides a base styling for most HTML elements. It makes use of an extensive list of components, some of which are drop-downs, navigation bars, and breadcrumbs. These components are made interactive with the numerous bundled JavaScript plugins.

JavaScript

JavaScript allows client-scripts to interact with the user, control the browser and alter the document content in real time. Along with HTML5, it creates an interactive and content-driven webpage.

AJAX

Asynchronous JavaScript and XML is a web development technique often implemented on the client side along with HTML and CSS. JavaScript uses it to transfer XML and other data to and from the web server asynchronously. This allows faster website interaction, as pages are not reloaded to display required content.

Web Framework and Database

After some research, we decided to use Django. It follows the Model-View-Controller (MVC) pattern. The controller is able to update the models’ states and sends commands to the view. The view then requests information from the model such as data structure, logic and business rules to proceed and generate output representation to the viewers. In addition, Django’s coding scheme enables the website to be built in phases. First, the database is set up, then the layout and UI is coded individually through its view and finally woven together through a regular-expression mapping system, which map URLs to function calls. This way, we can develop different chunks of the website and integrate them at the end rather than postpone the development because of a missing part of the site. However, to avoid being a data-driven website and follow the DRY principle, we have to identify our user behaviour and ensure that the user interaction with the overall website is effective, seamless and results-driven. Our approach is demonstrated in the navigation design above.

Moreover, Django was written in Python – our chosen back-end language. This means it shares Python's advantages, such as an array of libraries and third party packages. To fully take advantage of Django, the database will be designed and managed through its ORM instead of SQL. South – a third party library – will also be used for data migration.

Finally, Django has an extensible template language to integrate JavaScript, AJAX and jQuery while still separating design, content and Python code. It also provides an administrative interface, which further reduces the number of non-core development tasks.

Security and Risk Management Plan

Security Plan

CareSeek's security measures will be divided into two main components for development: web server security, and client-side and server-side security. Furthermore, there will be general measures taken such as keeping all software, libraries and frameworks at the most up-to-date stable versions, and regular peer code review sessions to detect any security holes or bugs that may be present.

Since the website will be small-scale (localised to Victoria), it is much more efficient to defensively program against currently-known and commonly-used threats rather than trying to focus on unknown attacks that will be inevitably harder to conceptualise and program against.

Web Server Security

To host our website, a trusted third-party hosting service will be used. This will provide high levels of security and require little effort to initialise and maintain, which meets the goal of a quick development lifecycle. A backup server will be run, in case the main server has a hardware failure or the web host coming under a denial of service (DoS) attack.

Client-Side and Server-Side Security

Each time a page containing dynamic content is loaded from the client side – for example, during account login or when user data is requested from a server – this creates an opportunity for sensitive information to be intercepted and for malicious code to be illegally injected. Hence, this web application must be actively defensive against such practices. The measures outlined below will be implemented to defend against common attacks.

Parameter Validation

All parameters such as search queries and information input will be passed to the server for storage and retrieval. To prevent SQL injections and cross-site scripting attacks, a validation check on all passed input will be developed. This will ensure no special characters such as script tags can be executed.

Another measure will be to only accept specific data for a given field. For example, if an email address is required, the input will be checked to ensure it is in the expected format. If a number or character is expected, then all other inputs will be rejected. Furthermore, a restriction on input length will be imposed – e.g. when searching for a carer, it is reasonable to assume that the search query will be less than 20 characters.

Access Control

To prevent bot access, passing a CAPTCHA test will be required during account creation and password or email change requests. In addition, there will be restrictions on the types of passwords accepted (e.g. requiring passwords to have a minimum of one number and capital letter), and the number of incorrect login attempts.

Anyone who wishes to use the site must have an account. A user will only be able to access their own data in write mode. All other data will be read-only, where appropriate. For example, a care seeker cannot see a carer's other shift details, apart from unavailable times shown by the shared calendar view. Furthermore, a user cannot access or modify the database directly. Queries will be handled client-side and implementation details will be hidden.

User login sessions will remain short to reduce the opportunity for unauthorised account access. A session will end if it is idle for a pre-defined period of time, or the browser is closed. This period will be optimally balanced between security and user convenience. When a session ends, the client-side cookies will be deleted and the server-side session marker will be cleared.

Data Encryption

Since the web application will be dealing with sensitive information (i.e employment contracts, addresses, phone numbers, passwords and emails), it will be necessary to hash it. This can be achieved with relative ease by using third-party Python libraries such as hashlib. On the client side, sensitive information will not be cached by the browser.

Response Sanitisation

Response sanitisation will involve checking that the requested process actually occurred to prevent malicious code execution. Any malicious activity detected will result in an internal server error that should not be seen on the client side. If the client find that the expected output was not generated, this will be an indication that access has been compromised.

Risk Analysis

Potential security issues that are most applicable to our web application have been tabled below. Given its small size and limited audience, it is unlikely that the more cunning attacks (e.g. DoS, SQL injections and scripting attacks) will be a major concern.

Category	Trigger	Likelihood	Impact	Risk	Contingencies
Confidentiality	SQL injection from poor or no input validation	Possible	Major	High	Take site offline to identify procedure call the breach has come from and quickly eliminate this security hole. If taking the site offline is too much of an inconvenience then we may put the site into a read-only mode In addition, scan the database to see if any data was accessed or modified. If so, recommend users to change passwords immediately. Change encryption keys and re-hash all data.
Confidentiality and Integrity	Malicious code run on the server resulting from no or poor input validation and/or process checking	Possible	Major	High	Take site offline to identify procedure call the breach has come from and quickly eliminate this security hole. If taking the site offline is too much of an inconvenience then we may put the site into a read-only mode In addition, scan the server to make sure that no malicious code has been installed and check sensitive data to see if anything was accessed or modified. If so, recommend users to change passwords immediately. Change encryption keys and re-hash all data.
Availability and Integrity	Server hardware failure and/or O/S crash	unlikely	Moderate	Low	Keep regular data backups and a second backup server online that traffic can be redirected to. Run a validation check on data to fix any corruption.
Availability and Integrity	Web Server downtime from maintenance or DDoS	unlikely	Moderate	Low	Have a second backup server running that traffic can be redirected to.

Authenticity and Confidentiality	Unauthorised user access resulting from identity theft or because sensitive data is being cached by the browser. User data may be modified and/or stolen	Possible	Major	High	Notify a user that their account has been compromised and block the user from logging in until that user has changed passwords Check the source of the id theft to make sure the browser is not caching sensitive session information Re-hash that affected user’s data.
Confidentiality	Access-level bugs resulting in accidental leak of private information – e.g. seeing another users contracts in full detail	Possible	Major	High	Peer reviewing code to make sure that there are no bugs in the access control resulting in the accidental leak of such information. Notify users to change passwords as a precaution.

Usability Testing Plan

Prior to the development of each major version or feature, a high-fidelity prototype will be created and the following usability test plan carried out.

Method

The chosen usability evaluation methods are lab observations and user reports (surveys and interviews).

The lab observation method was selected due to its flexibility, portability (does not require a usability lab), and the rich data captured. User reports was chosen because it is simple and cost-effective, yet yields unique data that supplements the lab observation.

Objectives

The group will assess whether participants successfully complete the tasks and how closely they follow the predetermined task steps. This will indicate the prototype's intuitiveness and usability, and the soundness of specific user interface (UI) decisions. If a particular error pattern emerged, this will guide further iterations.

Task completion time will be recorded to ascertain whether participants experienced difficulty with any of the tasks. Any errors will be described in detail and grouped into specific categories.

To further determine the usability and intuitiveness of the prototype, a survey and interview will be conducted. The survey and interview will contain questions regarding the prototype's effectiveness in meeting the predetermined goal.

Criteria

The criteria selected for the prototype assessment are users (a) complete each task (b) without any errors, and (c) within X minutes. The task time will be determined for each case by timing a group member performing the tasks, prior to familiarising themselves with the prototype.

To assist in the error analysis, the following error categories were decided upon:

i. Critical error – the participant requires the Evaluation Facilitator's assistance to continue with the task
ii. Non-critical error – the participant makes an initial mistake, but corrects it immediately
iii. External error – the participant does not read the task, or misunderstands it
iv. Prototype scope error – the participant attempts to use functionality beyond the implemented prototype scope

Data

Data points that help meet the objectives have been selected: task completion times, adherence to predetermined step flow, interview and survey answers, think-aloud data, and screencasts with audio and webcam video.

Task completion times will enable determination of difficult tasks. Step flow adherence will show common areas that require improvement or tasks that need modification. These data points support the objectives of determining the prototype's usability and intuitiveness, and the soundness of specific UI decisions.

The survey and interview answers will provide quantitative and qualitative data relating to the functionality, intuitiveness, and usability of the prototype. They will also help determine whether the design meets the intended goal.

Think-aloud data will indicate the participant's thinking during an error, which will assist in usability improvements and guide subsequent iterations – another objective. The screencasts with audio and webcam video will enable review of the tests and highlighting of any errors and other notable aspects.

Participants

For each test, two acquaintances that fit the demographics of a typical care seeker will be asked to participate, along with two that fit the demographics of a typical carer.

Materials

A webcam will be used to record the participants as they complete the tasks. Participants will use a group member's laptop to complete the tasks, which will also capture the screencast and webcam video. Observations and task step adherence will be recorded using pen and paper or typed on another laptop.

The second laptop will also be used for the survey and interview, and a mobile phone will record the interviews. The audio and video footage will be saved onto a USB drive.

Roles

Each group member has been assigned specific roles for the evaluation.

Daniel Esposito will be the Evaluation Facilitator. This involves welcoming the participant, informing them of the test, introducing the test aims and the prototype, providing instructions, informing them of the target user's profile, and receiving their consent for the audio-visual capture.

Hoang Nguyen will be the Error Observer. During the evaluation, she will check whether the participant followed the detailed task steps. If a specific step was not followed, she will note the action taken and any relevant think-aloud data.

Daniel Masters will be the Survey Facilitator/Interviewer. His role will involve guiding the participants through the survey, answering queries, and clarifying any questions. He will then ask follow-up questions regarding notable responses as well as perform the interview.

Project Timeline

Legend:	Daniel Esposito	Daniel Masters	Hoang Nguyen	Group

Week 1	Analyse the current situation and how we can address problem points	Market analysis and identification of potential competitors		
Week 2	Detail the project objectives, situational assessment, time constraints and budget constraints as initially addressed by the initial analysis	Analysis of team member skills to determine the areas each member is best suited to (i.e front-end, back-end, representative)		
Week 3	Research appropriate frameworks, software packages and API's that will be needed	Define internal and external dependencies		
Week 4	Team members engage in necessary research (jQuery, JavaScript, API, Django etc)	Proposal/pitch presentation	Finalise Project Proposal document	
Week 5		Formalise the data design, site map, and presentation design		
Week 6		Investigate common security practices for web applications and common security attacks		
Week 7	Detail the security implementations and risk management plans	Finalise web frameworks, database technology and other technologies that are going to be used and how these will interact with each other	Design a usability testing plan	
Week 8				Project plan/ application design submission and presentation
Week 9	Create all static pages that were detailed by the site-map	Database development to store all required data	Carer Search function, user registration, logon/logout and other database queries implemented server-side	
Week 10				
Week 11		Make web site dynamic pages by implementing JavaScript and jQuery – e.g. implementing button actions and event detection for registration, logon, logout, searching, changing user settings	Calendar implementation and booking system from both client and server perspective	
Week 12	Implement server-side security plans such as input sanitisation, user sessions etc			Bug testing, usability testing and final adjustments
Week 13	Prepare final report, reflect on the planning and design process and suggest adjustments			