Careerpilot data security and storage statement

Registered user details are held in a MySQL database on Catalyst 2's managed cloud servers. Passwords are encrypted using a one-way hashing algorithm using the PBKDF2 standard. Other security measures include output encoding, CSRF protection, XSS filtering, and protection from SQL injection.

1. Management of content and system access

All content for the website is managed internally by the Central Careerpilot Team (CCT) at the University of Bath via a content management system (CMS). The website CMS has various user privilege levels that allow access to certain parts of the website. All admin level user access is granted via the Central Careerpilot Team.

The user privilege levels are:

- Super user – access to everything on the site
- CMS users – access to amend any content within the website
- Adviser user – access to amend content within the adviser section of the website
- Provider content user – access to amend content within one or more provider/s section
- Job sector content user – access to amend content within the job sectors section
- Partner administrators - access to view career tools reports from specific school/s within their NCOP region
- Partner user – access to view career tools reports from their NCOP schools
- School administrators – access to view career tools reports from students within their school
- Teachers – access to view selected students within their school

2. Web design and development suppliers

The suppliers of the website are Float New Media Design Ltd (Float). Float is a UK registered privately owned and debt-free company based in Bath, UK. (www.floatdesign.net)

See relevant associated links for Float new Media Design

Quality Assurance Policy

http://www.floatdesign.net/company/quality-assurance-policy/

Service Level Agreement

http://www.floatdesign.net/company/service-level-agreement-(sla)/

Continuity if Float cease trading

In the event that Float cease trading, Float will ensure continuity by downloading all files and the database from the live server and passing these over to the Central Careerpilot Team. The hosting agreement that is currently between Float and Catalyst 2 will be transferred from Float and put into Careerpilot's name. The website will suffer no downtime as a result of this.

3. Core system code

Careerpilot is a bespoke system developed by Float New Media Design and built on the FUELPHP framework.

Fuel framework has implemented the following measures to ensure the safety and security within its web applications:

- Output encoding
- CSRF protection
- XSS filtering
- SQL injection

By default, Fuel doesn't filter POST and GET variables on input, and encodes everything on output. Fuel also encodes the URI when using URI segments, and escapes everything going into the database.

Output encoding

By default, Fuel favours output encoding to input filtering. The reason behind this is twofold. No matter where your data originates, and whether or not it is filtered, output encoding will make it harmless when it is sent to the client. It also means all input is stored in raw and unaltered form, so that no matter what happens, you will always have access to the original data.

CSRF Protection

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. The attack works by including a link or script in a page that accesses a site to which the user is known (or is supposed) to have been authenticated.

Fuel provides tools to protect forms against this kind of attacks, by including a security token in the form, which will can be validated upon form submission, and will ensure that when validated, the form was submitted by the client that has requested the form.

XSS filtering

Fuel provides XSS filtering using the HTMLawed library, a very fast and highly configurable library. By default it runs in safe and balanced mode.

Safe refers to HTML that is restricted to reduce the vulnerability for scripting attacks (such as XSS) based on HTML code which otherwise may still be legal and compliant with the HTML standard specs. When elements such as script and object, and attributes such as on mouseover and style are allowed in the input text, an input writer can introduce malevolent HTML code.

In balanced mode, HTMLawed checks and corrects the input to have properly balanced tags and legal element content (i.e., any element nesting should be valid, and plain text may be present only in the content of elements that allow them).

SQL injection

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application (like queries). The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of

vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.
This form of SQL injection occurs when user input is not filtered for escape characters and is then passed into an SQL statement. This results in the potential manipulation of the statements performed on the database by the end-user of the application. *source: Wikipedia*

Fuel protects against SQL injection by escaping all values passed to one of the Database class methods. Since this happens at the level of Fuel's central Query Builder, all code that uses the Query Builder, including Fuel's ORM package, will automatically use escaping.

4. SSL certificate

The website has a valid Comodo SSL certificate. Using an **SSL** certificate means that the information becomes unreadable to everyone except for the server to which the information is being sent therefore stopping any other computer intercepting the data.

5. Where the data is held

The website is hosted on a cloud server and is managed by Catalyst 2 (https://www.catalyst2.com/). Catalyst 2 is a UK registered privately owned and debt-free company.

For information on Catalyst 2's infrastructure please see the following link:

https://www.catalyst2.com/about-us/infrastructure/

Careerpilot Central Team
December 2023
University of Bath
Room WH 6.21
Claverton Down Road
Bath
BA2 7AY

Contact: careerpilot@bath.ac.uk

Helpline: 01225 386161
Float New Media Design Ltd
4 Miles Buildings
Bath
BA1 2QS