Careerpilot data security and storage statement

Registered user details are held in a MySQL database on United Hosting'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) 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
- NCOP user – access to view career tools reports from their NCOP schools
- NCOP administrators - access to view career tools reports from specific school/s within their NCOP region
- 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 United Hosting 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 to prevent nasty surprises 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 onmouseover 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 United Hosting (www.unitedhosting.co.uk). UnitedHosting is a UK registered privately owned and debt-free company. They have provided quality web hosting solutions with personal service since 1998.

Data centres

UnitedHosting operates from multiple datacentre locations in and around London. Their primary facility, named 'Centro', is conveniently located close to the M1 and M25, set within a secure private 50,000 sq ft compound. The datacentre boasts true enterprise specification with redundancy at every level of its design.

Data centre security

- 3m rota-spike security fence and perimeter anti ram barriers
- Blast proof anti-intruder shielded external windows and doors
- Proximity access locks on all external and internal doors
- Interlocked man-trap doors with biometric iris scanners to gain access into data floors
- Server cabinets have locked doors
- Perimeter and internal IP CCTV system monitored 24x7
- 24x7 on-site security guards with static and mobile patrols
- All on-site personnel are security vetted to BS7858 standard
- Only authorised security cleared staff are allowed into the facility

Offsite back ups

Using R1Soft Enterprise Server Backup software, United Hosting delivers Continuous Data Protection (CDP) for all customers, backing up data to an offsite location 4 times every day. A single file, MySQL database, entire site, or an entire server can be reliably recovered from a recent backup snapshot in a very short space of time.

Security Patches

Maintenance and security patches are applied at server level as and when required. United Hosting's security administrators manage this.

Accreditations

See appended document (UH-accreditations.pdf)

Careerpilot Central Team
January 2018
University of Bath
Widening Participation Office
Virgil Building
Bath
BA1 1JW
Contact: careerpilot@bath.ac.uk
Helpline: 01225 386161

Float New Media Design Ltd
5 Princes St,
Bath
BA1 2ED