Thrive-Online – Summary of Data Security Measures

The data provided by users of Thrive-Online is personal data and is subject to the General Data Protection Regulation 2018. Thrive (Fronting the Challenge Projects Ltd) is a Data Processor within the terms of the GDPR in respect of this data.
Thrive takes great care to ensure the confidentiality, integrity and availability of data and information processed on behalf of clients.

- Confidentiality: we take all reasonable steps to ensure that only those individuals who have a valid and authorised reason to access the information can do so.
- Integrity: we take all reasonable steps to ensure that information is not altered, deleted or otherwise modified by individuals or processes unauthorised to do so.
- Availability: we take all reasonable steps to ensure that the information can be accessed by the data owners when it is required.

Thrive-Online System Security

System Access

- Access via HTTPS only
- Approved login only
- Strong encryption (bcrypt) on passwords
- Strong encryption (bcrypt) on children's names
- Automatic screen block after 5 minutes
- Automatic logout after 30 minutes
- Adherence to OWASP Top 10

Hosting, Backup & Security Monitoring

- All application & back-up servers are held in secure data centres within the EU
- All servers have encrypted AWS EBS volumes
- All transfers of data between servers are encrypted using AES-256
- Separate back-ups are taken monthly, 30x daily and 6x hourly basis
- Dual systems for intrusion and detection monitoring are in place

System Administration

- The creation of administration users requires the authority of either the IT Services Manager, Chief Operating Officer or Managing Director and is audited regularly.
- All Thrive staff who have access to Thrive-Online are DBS checked.
- IT Support professionals are restricted from seeing any personal data unless they are DBS checked and specifically granted the right to do so by the IT Services Manager.

Security Testing

- Assessments and penetration tests are planned in response to:
  - System redevelopments and major upgrades
  - Ad-hoc events & checks
- Testing is carried out in accordance with the CREST standard with the aim of identifying security risks and vulnerabilities that could impact on confidentiality, availability or integrity of Thrive systems as well as the data contained within
- Company policy is to resolve any vulnerabilities exposed by testing within a tight timeframe:
  - Critical & high risk vulnerabilities are to be resolved immediately
  - Medium risk vulnerabilities are to be resolved immediately
  - Low risk vulnerabilities are to be resolved within the shortest time frame practicable
- Security assessments are provided by bona fide testing organisations with: ISO27001 certification; CHECK, TIGERSCHEME and/or CREST accreditation; industry recognised certificated employees.

Thrive is accredited with the Cyber Essentials Plus scheme