connect childcare
Outstanding Nursery Management Software

Connect Childcare's **GDPR** and **Security Process**

Here at Connect Childcare we take security and data protection very seriously. This document outlines our the processes that we use to ensure that we can comply with GDPR.

Policies

You can view our Data Protection Policy and Privacy Policy here. All of our policies are reviewed annually.

Organisational Security

Connect Childcare's CIO is accountable for the security of our organisation, with the Security Lead responsible for performing the day to day security activities.

Our Security Lead and Data Protection Officer can be contacted at dpo@connectchildcare.com or 01282 507 945.

No third parties have any access to customer data.

Physical & Environmental Security

Connect Childcare use an electronic key fob system to restrict access to the building reception, with a physical key required to gain entry to the office itself. Additionally, the server room access is limited to those who require access to perform their duties. We maintain a formal media destruction policy.

Our 3rd party data centres have very robust access control and protection from environmental hazards:

- Memset - https://www.memset.com/about-us/datacentre/
- Amazon - https://aws.amazon.com/compliance/data-center/data-centers/

Information Asset Classification and Control

We maintain a high level **Information Asset Register (IAR)** for all data we hold and the department responsible.

The classification of this data on the IAR is rated as low, medium or high.

- Low means that the data is available company wide, such as policies and training documents.
- Medium means that permission and specific job roles will have access to the data.
- High is the most sensitive data that is strictly need to know, such as customer data or HR documentation.

Any access is only given upon a business requirement that has to be approved by departmental heads and reviewed annually.

All data is kept within the UK for customers in the UK

- Memset data centres are located in Reading and Dunsfold
- We use London AWS region

Any data storage hardware that is used to store any customer data is destroyed as per our data destruction policy.

- Hardware that is being reused internally is given a single pass wipe before being reused
- Hardware that is leaving the company will undergo a three pass wipe to ensure that no data can be retrieved and is then physically destroyed to make it unusable.

Personnel Security

The terms and conditions of employment at Connect Childcare clearly state information security requirements, including non-disclosure provisions for both employees and contractors.
No third parties have any access to customer data.

Upon employment, all staff are given formal data protection and information security awareness training.

All employees and contractors are screened prior to employment:

- All references are checked.
- DBS checks are performed on all staff/contractors who have access to Connect Childcare Systems.
- Where access is required to high rated information, an enhanced DBS check is carried out.

Access Control

For internally facing applications, accounts are only granted on a business need. Passwords are subject to length requirements as per the NCSC guidelines: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

The Information Security Policy also dictates that passwords for each service is unique, and is stored within password management software.

Development & Maintenance

We use JIRA for development and QA ticket management and sprint planning. Our source control system allows for code review of all changes to our software, which allows a developer to flag up any concerns. Automated testing takes place upon each commit to our source control via a CI pipeline to ensure no current features are broken. OWASP ZAP is used to scan for common vulnerabilities.

All test data, whilst derived from customer data, is anonymised making it impossible to trace back to the original data subjects, but allows us to test real situations.

Our test systems are located within our offices (in secure racks). Developers are trained regarding common security issues to avoid, based on the OWASP top 10.

Information Security Incident Management

We have a dedicated team that are trained for responding to security incidents. All incidents are logged, and reported on with summaries provided to senior management to act upon. Any relevant policies, procedures and controls that relate to an incident are reviewed and updated if require to prevent a similar incident from happening again.

Penetration Testing

We undergo annual third party Penetration tests to ensure our internal testing is appropriate. We also perform regular internal tests with Security Specialists performing the role of the Red Team (Hackers).

Communication & Operation Management

All duties are segregated to their specific role, with a least privilege approach used to give only those required for the role.

Any changes to software developed are code reviewed by another member of the development team and passed through the QA team. Upon successful testing they are then rolled out to the live systems. Updates are performed outside of standard office / nursery operating hours to minimise impact to customers. Following on from deployment, checks are then performed to ensure a successful deployment with a rollback plan in place should there be an unexpected outcome.

Our servers are hosted by Memset & Amazon Web Services. Hosts are vetted by checking certifications held (ie, ISO 27001 / ISO 9001 / CE) with onsite visits if possible.

We protect our systems against newly discovered threats by:

- Performing weekly vulnerability scans
- Threat monitoring on platforms such as CISP
- Endpoint Security that is both signature and behaviour based.

Business Continuity Management/ Data Backups

We have documented processes for recovering from numerous scenarios which is based on existing processes which are used as part of our daily operations. The locations of our services and failover are in geographically distinct locations to prevent a single issue causing our services to drop.

We maintain backups of customer data for two weeks in three geographically distinct locations. Data is backed up every 15 minutes (and can be restored as such). It is stored in three geographically distinct locations. First it is stored in another data centre, and it is also stored on servers in our HQ in case both data centres are unavailable.

Compliance

Any exceptions to security policies and procedures are added to a risk register with full documentation and justification. Any employee found in non-compliance with security policies is subject to disciplinary action as per the company handbook.

Audits are performed annually

Connect are currently working towards Cyber Essentials with a long term aim of implementing ISO 27001. All our hosting providers are ISO 27001 certified.

The Connect Childcare system will provide functionality to allow our customers to comply with GDPR. This includes functionality to allow our customers (the data controller) to respond to data subjects' rights under the GDPR.

If you have any further questions relating to Connect Childcare's internal security and data protection processes, please contact our friendly team on:

01282 507 945