WOW World Group

Data Protection Policy
And
Data Protection Impact Assessment (DPIA)

DATA PROTECTION POLICY TABLE OF CONTENTS

1. POLICY STATEMENT

Wow World Group is committed to protecting personal data in accordance with:

The UK General Data Protection Regulation (UK GDPR)
The Data Protection Act 2018

We recognise that we primarily provide services to children under five years of age, and their families therefore apply enhanced safeguards to protect children's data.

2. PURPOSE

This policy establishes:

- How personal data is processed across Wow World Group
- How Head Office oversees compliance
- How franchisees manage local responsibilities
- How individuals' rights are protected

3. SCOPE

This policy applies to:

- Wow World Group
- All franchise locations
- All staff, directors, volunteers, and contractors
- All personal data processed in connection with WOW World Group's services

3.1 Definitions

Personal Data – Any information relating to an identifiable individual, such as name, address, date of birth, or contact details.
Special Category Data – Sensitive personal data, including health information, racial or ethnic origin, religious beliefs, or safeguarding information.
Criminal Offence Data – Data relating to criminal convictions or offences.
Processing – Any operation performed on personal data, including collection, recording, storage, use, disclosure, or deletion.
Controller – The person or organisation that determines the purposes and means of processing personal data.
Processor – Any person or organisation that processes personal data on behalf of a Controller.
Data Subject – The individual to whom the personal data relates.
Personal Data Breach – Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data.
Consent – Any freely given, specific, informed, and unambiguous indication of an individual's wishes by which they signify agreement to the processing of their personal data.
Parental Responsibility – Legal authority to provide consent for a child's data processing.

4. DATA PROTECTION BACKGROUND

UK data protection law governs how organisations collect, use, and protect personal data. Wow World Group processes data relating to children, families, and staff and ensures compliance with applicable legislation.

4.1 National Data Protection Law

Processing is governed by UK GDPR and the Data Protection Act 2018

4.2 UK GDPR

UK GDPR establishes principles, rights, and accountability requirements.

4.2.1 Personal Data

Includes but is not limited to:

- Child records
- Parent/guardian contact details
- Health information
- Safeguarding information
- Employment records

4.2.2 The Data Protection Principles

Wow World Group adheres to the seven principles of UK GDPR:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

4.3 Information Commissioner's Office

Wow World Group maintains registration with the Information Commissioner's Office (ICO) where required and cooperates fully with regulatory oversight.

As part of our franchise network:

- Individual franchisees act as Data Controllers and are responsible for also ensuring they register with the ICO.
- Franchisees must comply with all applicable data protection obligations, including responding to ICO requests, implementing appropriate safeguards, and maintaining accountability for the personal data they process locally.

- Wow World Group provides guidance and support to franchisees on ICO registration and compliance, but legal responsibility remains with the franchisee as the local Data Controller.

4.4 Data Protection Officer

Wow World Group Head Office has an appointed Data Protection Officer (DPO) in accordance with UK GDPR requirements. The DPO acts as a point of contact for all matters relating to the protection of personal data processed by the Group and franchise network.

The DPO's responsibilities include, but are not limited to:

- Monitoring compliance with UK GDPR, Data Protection Act 2018, and all internal data protection policies
- Advising franchisors and franchisees on data protection obligations and best practices
- Overseeing the implementation of Data Protection Impact Assessments (DPIAs) for high-risk processing activities
- Providing guidance on data subject rights, including access, rectification, and erasure requests
- Liaising with the Information Commissioner's Office (ICO) on matters of compliance or investigation
- Reviewing and reporting on data breaches, including notification requirements
- Ensuring staff and franchisees receive appropriate training on data protection and safeguarding
- Maintaining records of processing activities and monitoring retention and disposal practices

Franchisees must:

- Cooperate with the DPO in responding to queries or audits
- Notify the DPO promptly of any data breaches or incidents
- Seek guidance from the DPO where high-risk processing activities, such as handling children's or health data, are involved

4.41 Independence and Reporting

The DPO shall operate independently and report directly to the franchisor's senior management. The DPO is empowered to act without conflict of interest and may escalate issues as necessary to ensure compliance with data protection law.

The DPO's contact details are:
Name: Sean McKeon
Email: sean.mckeon@wowworldgroup.com

Franchisees and staff are encouraged to contact the DPO with any questions regarding the handling of personal data, including safeguarding concerns.

5 OBJECTIVES

Wow World Group aims to:

- Protect the personal data of children, families, and employees across all Wow World Group and franchise operations.
- Ensure lawful, fair, and transparent processing in line with UK GDPR and ICO guidance.
- Implement enhanced safeguards for children under five.
- Establish clear accountability across Wow World Group and franchisees, including their responsibilities as Data Controllers.
- Respond effectively to data breaches and data subject requests.
- Maintain staff and franchisee awareness and make training available on data protection via Wow Learning Hub.

6 GOVERNANCE PROCEDURES

6.1 Accountability & Compliance

Wow World Group demonstrates accountability by:

- Maintaining policies, procedures, and records of processing activities (ROPA).
- Conducting risk assessments, audits, and DPIAs.
- Monitoring franchisee compliance through their Franchisors.

Franchisees, as Data Controllers for data processed locally, are accountable for:

- Compliance with UK GDPR and the Data Protection Act 2018.
- Maintaining their own ROPAs where required.
- Ensuring staff are trained and aware of data protection obligations.
- ICO registration and cooperation with any regulatory oversight.

6.1.1 Privacy by Design

- Privacy safeguards are embedded into new systems and processes at both Wow World Group and franchise locations.
- Data collection is minimised and only what is necessary is processed.
- Franchisees must implement privacy-by-design measures locally.

6.1.2 Information Audit

Wow World Group conducts regular audits of central operations.

Franchisees must:

- Conduct local audits of personal data processing.
- Ensure compliance with retention schedules, security measures, and legal obligations.
- Report audit findings to Wow World Group upon request.

6.2 Legal Basis for Processing

All processing is conducted on a lawful basis under UK GDPR, including:

- Contractual obligation
- Legal obligation

- Legitimate interests
- Consent
- Vital interests

Franchisees must ensure local lawful bases are clearly documented and applied.

6.2.1 Processing Special Category Data

- Special Category Data, including safeguarding and health records, are processed only with appropriate legal conditions.
- Franchisees must ensure limited access, lawful processing, and secure storage for local special category data.

6.2.2 Records of Processing Activities

- Wow World Group maintains central ROPA for corporate processing.
- Franchisees must maintain ROPA for all local data processing and provide access to Wow World Group on request.

6.3 Codes of Conduct & Certification

- Franchisees are expected to follow industry codes of conduct and comply with ICO guidance.
- Wow World Group provides guidance, but franchisees remain accountable for local compliance.

6.4 Data Retention & Disposal

Wow World Group shall establish and maintain a Group Data Retention Framework, which shall provide that Customer Personal Data processed via the Booking System is retained for a period of six (6) years following the end of the relevant customer relationship or last interaction, unless a longer retention period is required by applicable law, safeguarding obligations, or insurance requirements.

Franchisees shall comply with the Group Data Retention Framework and shall not retain Personal Data for longer than six (6) years after the end of the customer relationship, save where retention is required by law or regulatory obligation.

Franchisees are responsible for implementing and operating local retention procedures consistent with the Group Data Retention Framework, including:

- Secure deletion or anonymisation of Personal Data upon expiry of the applicable retention period;
- Ensuring deletion methods are appropriate to the nature of the data; and
- Maintaining appropriate records of disposal activities where required.

All deletion and disposal activities must comply with applicable data protection legislation, safeguarding requirements, and relevant insurance obligations.

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Wow World Group has completed a Data Protection Impact Assessment (DPIA) for the central franchise booking system, in accordance with Article 35 UK GDPR. The DPIA assesses risks to individuals' rights and freedoms arising from the collection and processing of personal data, including children's data and health information, and identifies appropriate mitigation measures.

The DPIA covers all personal data processed via the booking system, including:

- Customer names, dates of birth, and gender
- Medical or health information
- Booking and attendance records
- Marketing consent and preferences
- Parent/guardian contact details

7.1 Roles & Responsibilities

Wow World Group:

Maintains and updates the DPIA
Ensures system-wide security, retention, and consent measures are implemented
Reviews risks associated with system changes, analytics, or new data fields

Franchisees

Follow the DPIA's measures when processing local customer data
Notify the franchisor of any incidents, local risks, or changes affecting the system

7.2 Risk Management & Mitigation

The DPIA identifies and addresses high-risk areas, including:

Special category data (medical/health)
Data relating to children
Centralised access and processing
Retention and secure disposal
All staff and franchisees must follow the measures outlined in the DPIA to minimise risk.

7.3 Review & Update

The DPIA is reviewed annually, or sooner if there are significant changes to the system, processes, or data categories. Updates are communicated to all franchisees, and compliance with the DPIA is mandatory. The full DPIA document is maintained separately as a formal record and can be accessed by authorised staff and franchisees for compliance and audit purposes.

8 DATA SUBJECT RIGHTS PROCEDURES

- Wow World Group coordinates responses for centrally processed data.
- Franchisees, as local Data Controllers, are responsible for responding to data subject requests regarding data they control.

Rights include:

- Access to personal data
- Rectification of inaccurate data
- Erasure (subject to legal obligations)
- Restriction of processing
- Objection to processing
- Data portability
- Withdrawal of consent

Requests must be responded to within one calendar month. Franchisees must escalate complex requests to Wow World Group.

8.1 Consent & Right to be Informed

- Consent must be freely given, specific, informed, and unambiguous.
- Franchisees must obtain parental consent for children where required and maintain records locally.

8.1.1 Consent Controls

- Consent must be auditable and withdrawable at any time.

8.1.2 Child's Consent

- Children under 13 cannot provide legal consent; parental consent is required.

8.1.3 Alternatives to Consent

- Where consent is not appropriate, other lawful bases must be documented.

8.1.4 Information Provisions

- Parents and guardians must be provided with clear, plain-English privacy information at franchise locations and Wow World Group.

8.2 Privacy Notice

- Wow World Group provides template Privacy Notices.
- Franchisees must ensure Privacy Notices are displayed, issued to parents, and accessible for local processing.

8.3 Personal Data Not Obtained from the Data Subject

- Individuals must be informed within statutory timelines when data is collected from third parties.
- Franchisees must implement this locally for all non-directly obtained data.

8.4 Right of Access

- Wow World Group handles central requests; franchisees handle local requests.

8.4.1 Subject Access Requests

- Identity verification required.
- Responses issued within one month.
- Franchisees escalate complex or high-risk requests to Wow World Group.

8.5 Data Portability

- Applicable to automated processing where consent or contract is the basis.
- Franchisees ensure local systems allow portability where applicable.

8.6 Rectification & Erasure

8.6.1 Correction of Data

- Inaccurate or incomplete data must be corrected promptly.

8.6.2 Right to Erasure

- Data is erased upon request unless legal obligations require retention.
- Franchisees must implement local erasure procedures.

8.7 Right to Restrict Processing

- Franchisees must comply with local requests to restrict processing.

8.8 Objections & Automated Decision Making

- Individuals may object to processing on legitimate interest grounds.
- No automated decisions with legal or significant effects are applied to children.

9 OVERSIGHT PROCEDURES

- Wow World Group monitors central operations and provides guidance.
- Franchisees are accountable for local oversight, including compliance, staff training, ICO obligations, and data security.

9.1 Security & Breach Management

- Access controls, secure storage, encryption, and staff confidentiality are mandatory.
- Breaches must be reported immediately to Wow World Group.
- Franchisees are responsible for reporting local breaches to Wow World Group and, where required, to the ICO within 72 hours.

10 TRANSFERS & DATA SHARING

- No personal data leaves the UK without adequacy decisions or appropriate safeguards.
- Franchisees are responsible for ensuring local data sharing complies with UK GDPR and ICO requirements.

11 AUDITS & MONITORING

- Wow World Group audits central operations and provides guidance.
- Franchisees are accountable for local audits and must provide evidence of compliance, including ICO registration, retention, and processing practices.

12. TRAINING

Wow World Group Head Office shall develop, maintain, and provide:

- Induction data protection training for all new staff
- Annual refresher training on data protection and safeguarding
- Enhanced training for processing children's data and special category (health) data

12.1 Delivery and Compliance by Franchisees

Franchisees are responsible for:

- Ensuring that they and all local staff who have access to customer data complete Data Protection training within required timeframes
- Maintaining accurate records of training completion, including dates and participants
- Ensuring that staff understand and comply with all policies, procedures, and safeguards associated with the Booking System

12.2 Monitoring and Audit

Wow World Group reserves the right to:

- Audit franchisee training records periodically
- Require remedial training where compliance gaps are identified
- Update training content and policies to reflect legal or operational changes

13. PENALTIES

Failure to comply with this policy may result in:

- Disciplinary action (for employees)
- Contractual consequences for franchisees
- Legal action or regulatory penalties, including ICO fines

Franchisees remain accountable as local Data Controllers for regulatory compliance.

14. RESPONSIBILITIES

Role	Responsibility
Board of Directors	Overall accountability for Wow World Group compliance
Wow World Group Head Office / DPO	Governance oversight, guidance, training, and central monitoring
Franchisees	Local compliance, ICO registration, retention/deletion, data subject requests, staff training
All Staff	Adherence to this policy and reporting breaches

Data Protection Impact Assessment (DPIA)
Franchise Booking System Wow World Group

This document provides a central reference for the franchise booking system, GEMA and outlines how personal data is processed, risks assessed, and mitigation measures implemented. It is intended for reading and operational guidance.

The franchise booking system, GEMA collects and processes the following categories of personal data:

- Children's information: name, date of birth, gender
- Medical or health information (special category data)
- Parent/guardian contact details
- Booking and attendance records
- Marketing consent and preferences
- Payment information (non-card data only)

Data subjects: children attending classes, their parents/guardians, and adult customers.

Purposes:

- Class bookings and attendance management
- Safeguarding and safety of participants
- Communication with customers
- Compliance with insurance obligations
- Network reporting and brand oversight

Lawful basis:

- Article 6 UK GDPR – Contract, Legitimate Interests, Legal Obligation
- Article 9 UK GDPR – Explicit consent or safeguarding requirements

Why a DPIA Was Completed

A DPIA was undertaken because the system processes:

- Special category data (health/medical information)
- Children's data (vulnerable individuals)
- Centralised, mandatory processing across multiple franchisees
- Large-scale potential impact in the event of a data breach

This ensures compliance with UK GDPR Article 35 and demonstrates accountability.

Key Risk Areas and Mitigations

Risk	Mitigation Measures	Residual Risk
Unauthorised access to children's data	Role-based access; encryption; audit logs	Low-Medium
Breach of health/medical data	Encryption at rest/in transit; secure system; breach response plan	Low-Medium
Excessive retention	Data retained **6 years** after customer relationship; automated deletion enforced	Low
Inadequate consent	Standardised consent wording; staff training	Low

Other mitigations:

- Staff training for handling children's and health data
- Clear joint controller responsibilities
- Documented deletion and retention procedures
- Annual review of processing and DPIA

Staff Guidance

Franchisees should:

- Ensure any staff with access to this data are aware of DPIA measures
- Follow the central policy for processing personal data
- Maintain local compliance with retention and secure deletion rules
- Refer to the DPIA for guidance on high-risk data handling

This reference DPIA is reviewed annually or if system changes occur (e.g., new data fields, analytics, or retention changes). Franchisees are expected to comply with updated measures