



1801Adventures GDPR and Data Handling Policy

Purpose and scope

This Privacy Policy explains **what personal data 1801Adventures collects**, **why** we process it, **how long** we keep it, **who** we share it with, and **how** you can exercise your rights. It applies to all visitors, subscribers, customers, and users of 1801Adventures services and websites. **Controller:** [1801Adventures — Andrew Grange, Aberdovey Dr, Stockon-on-Tees, 1801adventures@gmail.com].

Personal data collected and lawful bases

Categories of data we collect: contact details (name, email), account and subscription data, payment metadata (processor reference only), support correspondence, Discord identifiers, analytics data (IP, device, cookies), and optional profile content you provide. **Lawful bases:** performance of contract (subscriptions, fulfilment), legitimate interests (fraud prevention, service improvement), and consent (marketing communications and non-essential cookies). For each processing activity we record the specific lawful basis and make it available on request.

Data subject rights and how to exercise them

You have the right to **access, rectify, erase, restrict, object**, and **port** your personal data, and the right to withdraw consent where processing relies on consent. If you request deletion after consenting to immediate access to digital content, refunds or access removal may apply under the Consumer Contracts Regulations; we will explain consequences at point of consent. To exercise rights, contact **1801adventures@gmail.com**; we will acknowledge requests within **one month** and comply or explain any lawful refusal.

Sharing, transfers, retention

We share data only with named processors necessary to deliver services: **Memberful (payments/subscriptions)**, **Discord (calls,messaging)**, **Hostinger (Hosting provider)**, **Wordpress (Website handling)**, **Google (SEO and data analytics)**, **Mailerlite (Newsletter, marketing communications)**, **Startplaying.games (Game sign up/payment handling)**. Each processor acts under contract and appropriate safeguards. **Retention:** Please see appendix 1.1 covering data retention.

**Security, breaches and accountability**

We implement **appropriate technical and organisational measures** (encryption at rest/in transit, access controls, regular backups, least-privilege access). In the event of a personal data breach that risks individuals' rights, we will notify the ICO **without undue delay** and affected individuals where required by law. We maintain records of processing activities and conduct periodic DPIAs for high-risk processing.

Contact, complaints and updates

Contact: 1801adventures@gmail.com. You may also complain to the UK Information Commissioner's Office (ICO) if you remain dissatisfied. We review and update this policy as required; the current version date appears at the top of the document.



Appendix:

1.1 Data Retention Table

Category of personal data	Examples	Retention period
Account and subscription data	Name, email, Memberful account ID, subscription status	While account is active + 2 years
Billing and payment records	Invoices, payment references, refunds (payment processor stores card tokens)	6 years (for tax and accounting compliance)
Support and correspondence	Email support threads, helpdesk tickets, Discord support messages	2 years after last contact
One-to-one call scheduling data	Agreed call times, Discord IDs, call notes (non-sensitive)	12 months after call date
Marketing consent & preferences	Opt-in records, marketing consents, unsubscribe logs	Until consent withdrawn + 2 years
Analytics and usage data	IP (anonymised where possible), page views, device info, cookies	12 months (or per analytics provider settings)
Cookies and tracking	Consent records and cookie identifiers	Consent record: until withdrawn; cookie data: per cookie expiry
Downloaded content logs	Records of which subscriber downloaded which asset	12 months after download
Backups and logs	System backups, server logs (may contain personal data)	30–90 days (or as per hosting provider policy)
Legal and compliance records	Complaints, DSR logs, contract records	6 years (or longer if required by law)
Deleted accounts	Minimal archival record to prevent re-registration fraud	2 years (or as required for fraud prevention)