Unigold 2000 Limited – Data Protection Policy (UK GDPR)

Updated: February 2026

1. Introduction

This Policy sets out the obligations of Unigold 2000 Limited (company number 03225642), whose registered office is 256 High Street, Guildford, Surrey, GU1 3JG (the 'Company'), regarding data protection and the rights of customers, staff and business contacts ('data subjects') under the UK General Data Protection Regulation ('UK GDPR') and the Data Protection Act 2018. It replaces earlier versions that referenced the EU GDPR.

The Company is committed to lawful, fair and transparent processing and places high importance on the correct handling of personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

2. The Data Protection Principles

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in a form permitting identification for no longer than is necessary.
- Processed in a manner ensuring appropriate security (integrity and confidentiality).

3. The Rights of Data Subjects

- Right to be informed (privacy information).
- Right of access (subject access request).
- Right to rectification.
- Right to erasure (right to be forgotten).
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Rights in relation to automated decision-making and profiling.

4. Lawful, Fair and Transparent Processing

Processing is lawful only if at least one lawful basis applies: consent; contract; legal obligation; vital interests; public task; or legitimate interests. For special category data, an additional condition under Article 9 UK GDPR (and Schedule 1 of the Data Protection Act 2018, where applicable) is also required.

5. Specified, Explicit and Legitimate Purposes

Personal data is collected and processed for purposes described in our Privacy Notice and Records of Processing Activities (ROPA). Data subjects are informed at the time of collection or within one month where obtained from third parties.

6. Adequate, Relevant and Limited Data Processing

We collect and process only the personal data necessary for each specified purpose.

7. Accuracy and Keeping Data Up to Date

We take reasonable steps to keep personal data accurate and up to date and rectify inaccuracies without delay.

8. Data Retention

We retain personal data only for as long as necessary for the purposes collected, in line with our Data Retention Policy. When no longer required, data is securely deleted or anonymised.

9. Secure Processing

We apply appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10. Accountability and Record-Keeping

The Company keeps internal records of processing activities (ROPA) including purposes, categories of data and data subjects, recipients, international transfers, retention periods and security measures.

Data Protection Officer (DPO): Matthew Gaskin (ICO registration number Z2857312).

11. Data Protection Impact Assessments (DPIAs)

We conduct DPIAs for high-risk processing, including the use of new technologies or monitoring activities, assessing necessity, proportionality, risks and mitigations.

12. Keeping Data Subjects Informed

We provide clear privacy information including identity and contact details, purposes, lawful bases, categories collected, recipients, international transfers, retention, rights, the right to complain to the ICO, and whether provision of data is a statutory/contractual requirement. Where data is obtained from third parties, information is provided within one month or at first contact, or before disclosure to another recipient, whichever is earlier.

13. Data Subject Access

Data subjects can make Subject Access Requests to obtain a copy of their personal data. We respond without undue delay and within one month of receipt (extendable by up to two further months for complex or numerous requests). We do not charge a fee unless a request is manifestly unfounded or excessive.

14. Rectification of Personal Data

We rectify inaccurate personal data without undue delay and notify recipients where feasible.

15. Erasure of Personal Data

We erase personal data upon valid request where applicable (e.g., no longer necessary, consent withdrawn, successful objection, unlawful processing, or to comply with a legal obligation).

16. Restriction of Processing

We restrict processing upon valid request and notify recipients where feasible.

17. Data Portability

Where processing is based on consent or contract and carried out by automated means, we provide personal data in a structured, commonly used and machine-readable format and, where technically feasible, transmit it directly to another controller at the data subject's request.

18. Objections to Processing

We stop processing upon objection to direct marketing. For other objections based on legitimate interests or public task, we stop unless we demonstrate compelling legitimate grounds or the processing is for legal claims.

19. Automated Decision-Making and Profiling

We do not use personal data for solely automated decisions that produce legal or similarly significant effects without appropriate safeguards. Where such processing applies, individuals can obtain human intervention, express their point of view, and contest decisions.

20. Data Security – Transferring Personal Data and Communications

Personal data is transmitted using secure channels (e.g., encrypted email or files). Where hard copy transfer is necessary, it is sealed and marked confidential. Fax transmission is avoided unless strictly necessary and subject to pre-notification and secure receipt.

21. Data Security – Storage

Electronic personal data is stored securely using access controls and encryption where appropriate. Hard copy records are stored in locked storage. Backups are encrypted and tested. Mobile and BYOD use is controlled; storage on personal devices is prohibited unless explicitly authorised and subject to safeguards.

22. Data Security – Disposal

Personal data is securely deleted or destroyed when no longer required, in accordance with our Data Retention Policy.

23. Data Security – Use of Personal Data

Access to personal data is on a need-to-know basis. Screens must be locked when unattended. Marketing uses comply with PECR and UK GDPR consent requirements.

24. Data Security – IT Security

Strong, unique passwords and MFA are used where available. Systems are kept up to date with security patches in a timely manner subject to change management. Software installation on Company devices requires approval.

25. Organisational Measures

All personnel handling personal data are trained and aware of responsibilities. Access is limited to those who need it. Processing methods are reviewed regularly. Contractors are bound by equivalent obligations and appropriate data processing terms.

26. International Transfers

Personal data is primarily stored and processed in the UK and/or EEA. Where transfers outside the UK occur, we implement appropriate safeguards such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, or rely on another lawful transfer mechanism. We assess destinations for adequacy and conduct transfer risk assessments where appropriate.

27. Personal Data Breach Notification

All suspected personal data breaches must be reported immediately to the DPO. Where a breach is likely to result in a risk to individuals' rights and freedoms, the ICO will be notified without undue delay and, where feasible, within 72 hours of awareness. Where a breach is likely to result in a high risk, affected individuals will be informed without undue delay.

28. Implementation and Review

This Policy is effective from 1 January 2018 and is reviewed at least annually or upon material change in processing or law. The current version was updated on 9 February 2026.

Approved by: Matthew Gaskin, Managing Director / Data Protection Officer