Goldphish Privacy Policy

We believe privacy notices should be readable. This one is. Each section has a plain English summary in italics, followed by the full legal detail. The plain English summaries are provided for convenience only — the legal text governs in the event of any inconsistency.

If you have any questions about this policy or how we handle your data, contact us at info@goldphish.com.

---

1. Who We Are

Plain English: *We're Goldphish — a UK company that makes security awareness training and simulated phishing software, sold primarily through MSP and MSSP partners. This policy covers how we handle personal data across our marketing website and our platform. We are registered with the ICO as required under UK data protection law.*

Goldphish is the trading name of GOLDPHISH LTD, a company incorporated in England and Wales under company registration number 10333752.

Registered address: Dalton House, 60 Windsor Avenue, London, SW19 2RR, United Kingdom.

Data protection contact: info@goldphish.com

ICO Registration Number: ZA276913

References to "Goldphish", "we", "us", or "our" refer to GOLDPHISH LTD.

This Privacy Policy applies to:

- Visitors to our marketing website at www.goldphish.com
- Users of the Goldphish platform at app.goldphish.com
- Sales partners, resellers, and prospective partners
- Suppliers
- Business contacts and prospective customers
- Subscribers to the Go Phish newsletter

Children and minors: The Goldphish platform and marketing website are not directed at individuals under the age of 18. We do not knowingly collect or process personal data relating to children. If you believe we have inadvertently collected data relating to a minor, please contact us at info@goldphish.com and we will delete it promptly.

---

2. Our Role: Controller and Processor

Plain English: *Depending on the context, we play different roles under data protection law. When you visit our website, sign up for marketing, or engage with us commercially — we control your data and this policy applies in full. When your employer or MSP uses the Goldphish platform and you're an end user of it — we process your data on their behalf, and their privacy notice governs alongside ours. The legal terms for this are set out in our*

Data Processing Agreement, which forms Schedule 1 of our platform Terms of Service.

Data protection law distinguishes between a **data controller** (who decides why and how personal data is processed) and a **data processor** (who processes data on a controller's instructions).

Where Goldphish is the controller: When we collect and process personal data directly — including website visitors, business contacts, prospective customers, partners, and suppliers — Goldphish acts as the data controller. This policy sets out your rights and our obligations in full.

Where Goldphish is the processor: When an MSP, MSSP, or direct customer deploys the Goldphish platform and their employees or end users interact with it, Goldphish acts as a data processor on that customer's instructions. In this context, the customer organisation is the data controller. Our obligations as processor are governed by our Data Processing Agreement (DPA), which forms Schedule 1 of the Goldphish platform Terms of Service.

If you are an end user of the Goldphish platform and have questions about how your employer or their MSP handles your data, please contact them directly.

---

3. What Data We Collect and Why

Plain English: *We only collect what we actually need, and we're clear about why. This section breaks down who you are — website visitor, platform user, partner, supplier, prospect, or newsletter subscriber — and tells you exactly what we hold and what we use it for.*

We collect and process different personal data depending on your relationship with us. The sections below set this out by category.

3a. Website Visitors

Plain English: *When you browse our website, we collect basic technical data automatically — things like your IP address and which pages you visited. We use this to understand how the site is being used and to keep it running properly. We don't use it to identify you personally.*

When you visit www.goldphish.com, we may automatically collect:

- IP address
- Browser type and version
- Pages visited and time spent
- Referring URL
- Device type and operating system

Legal basis: Legitimate interests — specifically, maintaining the security and performance of our website and understanding how it is used in aggregate.

Retention: Anonymised analytics data is retained for up to 26 months. Raw access logs are retained for up to 90 days.

3b. Website Enquiries and Contact Forms

Plain English: *If you fill in any form on our website — whether that's a contact form, a free trial request, a partner enquiry, or a quote request — we collect the details you submit and use them to respond to you. We may also follow up with relevant information about Goldphish. You can ask us to stop at any time.*

When you submit a form on our website, we collect:

- Name
- Email address
- Company name
- Job title or role
- The content of your enquiry

Legal basis: Legitimate interests — responding to your request and managing our business relationship with you.

Retention: Up to three years from our last contact with you, unless you request earlier deletion.

We may use third-party tools including HubSpot to manage and track responses to website enquiries.

3c. Platform Users

Plain English: *If you use the Goldphish platform — because your employer has deployed it — we hold data about you to run the service. This includes your name, email, and your results from phishing simulations and training modules. The platform records your activity automatically, including whether you clicked a simulated phishing email, and may direct you to training content as a result. This is not a risk score or a formal profile — it's how the training works. Your employer or their MSP can see this data on their dashboard. Any decisions they make based on it are theirs, not ours.*

As a user of the Goldphish platform, we hold and process the following data:

- Name
- Email address
- Password (stored in hashed form — we cannot read it)
- Employer
- Employee department
- Location (country and time zone)
- Responses to phishing simulation exercises
- Results from learning module assessments
- Completion progress data
- IP address
- Any personal data accessed via third-party integrations activated by your employer
- User identifiers on third-party accounts integrated with Goldphish

Legal basis: Processing is carried out on behalf of your employer (the data controller) under our Data Processing Agreement. Where Goldphish has an independent legal basis, this is legitimate interests — specifically, the performance of our contract with

your employer, platform security, and product improvement using anonymised data.

Automated processing: The Goldphish platform includes automated just-in-time training. If you interact with a simulated phishing email, you may be automatically directed to a training module without human intervention. This automated action is remedial in nature — it is designed to provide immediate learning, not to penalise or make decisions about you. The platform also records individual activity data including phishing simulation results, training completion rates, and assessment scores. This data is visible to your employer or their MSP as the data controller. Any employment or performance decisions made on the basis of this data are the responsibility of your employer, not Goldphish.

Retention: For the duration of our contract with your employer. All personal data is deleted within 90 days of contract termination.

3d. Sales Partners and Resellers

Plain English: *If you're a partner or reseller working with Goldphish, we hold basic contact information about you to manage our commercial relationship. We keep this for seven years after the contract ends, in line with standard UK business record-keeping requirements.*

As a partner or reseller of Goldphish, we hold:

- Name
- Contact details
- Job title

Legal basis: Legitimate interests — fulfilling our business-to-business contract with your organisation.

Retention: Up to seven years from contract termination, unless you request earlier deletion. Data is irreversibly deleted at that point.

3e. Suppliers

Plain English: *If you supply goods or services to Goldphish, we hold your contact and payment details to manage that relationship and meet our financial record-keeping obligations.*

As a supplier to Goldphish, we hold:

- Name
- Contact details
- Bank details

Legal basis: Legitimate interests — fulfilling our contract with you and meeting legal financial record-keeping obligations. We cannot continue our contractual relationship if we cannot process this data.

Retention: Up to seven years from contract termination, or longer where required by law

for financial records. Data is irreversibly deleted at that point.

3f. Business Contacts and Prospective Customers

Plain English: *If we have your details because you expressed interest in Goldphish, attended an event, or were introduced to us as a potential customer — we hold that information to stay in touch and share relevant content. You can ask us to stop at any time, and we'll remove you promptly.*

As a business contact or prospective customer, we hold:

- Name
- Contact details
- Job title or description
- Company
- Location

Legal basis: Legitimate interests — business communication and B2B marketing.

This data may have come directly from you, or from a reputable data-as-a-service provider. Where data has been sourced from a third party, we take reasonable steps to ensure that sourcing was lawful.

Retention: Up to three years from our last contact with you, unless you request earlier deletion. Data is irreversibly deleted at that point.

3g. Newsletter Subscribers

Plain English: *If you subscribe to our Go Phish newsletter, we hold your email address and use it to send you the newsletter. That's it. You can unsubscribe at any time using the link in any newsletter email, and we'll stop immediately.*

We publish the Go Phish newsletter via Beehiiv. When you subscribe, we collect:

- Email address
- Name (if provided)

Legal basis: Consent — you have actively opted in to receive the newsletter. You can withdraw your consent at any time by clicking the unsubscribe link in any newsletter email, or by contacting us at info@goldphish.com. Withdrawal of consent does not affect the lawfulness of any processing carried out before withdrawal.

Retention: For as long as you remain a subscriber. On unsubscription, your data is deleted from our active subscriber list within 30 days.

The newsletter is managed via Beehiiv. By subscribing, your email address will be processed by Beehiiv in accordance with their own privacy policy, available at www.beehiiv.com/privacy.

3h. Recorded Calls

Plain English: *We may record calls for training and service improvement purposes. We'll always tell you at the start of a call if it's being recorded, and you can ask not to be recorded.*

Where calls are recorded for training, service improvement, or customer support purposes, this is subject to consent, strict access controls, and appropriate security protections.

Retention: Up to three years, then irreversibly deleted.

4. Cookies and Tracking Technologies

Plain English: *Our website uses cookies — small files stored on your device — to make the site work properly and to understand how it's being used. You can control which cookies you accept. We'll always ask before we set anything that isn't strictly necessary.*

Our website uses the following categories of cookies:

- **Strictly necessary cookies:** Required for the website to function. These cannot be disabled.
- **Analytics cookies:** Used to understand how visitors interact with the website — which pages are visited, how long people stay, where they arrive from. This data is aggregated and anonymised. We use tools including Google Analytics for this purpose.
- **Functional cookies:** Used to remember your preferences and improve your experience on the website.
- **Marketing cookies:** Used to deliver relevant content and measure the effectiveness of our marketing. These are only set with your consent.

You can manage your cookie preferences at any time via the cookie settings on this website. You can also manage cookies through your browser settings, though disabling certain cookies may affect how the website functions.

For more information about cookies generally, visit www.allaboutcookies.org.

---

5. Third-Party Services

Plain English: *We use a small number of trusted third-party tools to run our business. We don't sell your data to anyone. Where your data goes to a third party, it's to provide a service to you or us — nothing else.*

We use the following third-party services which may process personal data on our behalf:

- **IONOS** — Cloud server and data centre hosting
- **Google LLC** — Administrative and cloud storage services
- **Help Scout PBC** — Customer support
- **HubSpot Inc.** — Customer relationship management and marketing
- **Mailgun Technologies Inc.** — Transactional email delivery
- **Beehiiv Inc.** — Newsletter publishing and distribution

- **Xero Limited** — Accounting and billing

We only transfer personal data to third parties that comply with applicable data protection law. We do not sell personal data to any third party. Data used for aggregated analysis or market research is anonymised before use and cannot be used to identify individuals.

This list is reviewed periodically. If you would like up-to-date information on the third-party processors we use, please contact us at info@goldphish.com.

---

6. International Data Transfers

Plain English: *Some of the third-party tools we use are based outside the UK, which means your data may be processed in other countries. We only allow this where there are proper legal safeguards in place. For data flows between the UK and EU, the UK holds full adequacy status — meaning data can flow freely without additional legal steps.*

Where personal data is transferred outside the United Kingdom, we ensure that appropriate safeguards are in place in accordance with UK GDPR. These may include:

- Transfers to countries with an adequacy decision from the UK Secretary of State
- Standard contractual clauses approved for use under UK GDPR
- Binding corporate rules or other approved transfer mechanisms

The United Kingdom holds an adequacy decision from the European Commission (renewed December 2025, valid until December 2031), meaning personal data can flow freely between the EU/EEA and the UK without additional transfer mechanisms.

For details of the specific safeguards in place for any particular transfer, please contact us at info@goldphish.com.

---

7. Data Security

Plain English: *We take reasonable technical and organisational steps to protect your data. No system is completely immune to risk, but we take this seriously. Our Security Measures page at www.goldphish.com/security-measures sets out the specific controls we apply to the Goldphish platform.*

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, accidental loss, destruction, or damage. These include access controls, encryption in transit, hashed password storage, and regular security reviews.

Transfers of data over the Internet carry inherent risks. While we take all reasonable precautions, we cannot guarantee absolute security of data in transit. Platform users are responsible for keeping their own login credentials secure and for notifying us promptly if they suspect any unauthorised access.

---

8. Data Breach Notification

Plain English: *If there's ever a data breach that affects your rights or freedoms, we'll tell the ICO within 72 hours and notify you without unnecessary delay if you're at high risk. We won't sit on it.*

In the event of a personal data breach, we will:

- Notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects.
- Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

---

9. Your Rights

Plain English: *You have real rights over your personal data — not just the right to be told about it, but the right to access it, correct it, delete it, or object to how it's being used. If something doesn't feel right, come to us first — we'd rather resolve it directly than have you go straight to the regulator. But if you're not satisfied, the ICO is always available to you.*

Under UK GDPR, you have the following rights in relation to your personal data:

- **Right of access** — to request a copy of the personal data we hold about you
- **Right to rectification** — to ask us to correct inaccurate or incomplete data
- **Right to erasure** — to ask us to delete your data in certain circumstances
- **Right to restriction** — to ask us to limit how we use your data in certain circumstances
- **Right to object** — to object to processing based on legitimate interests, including for direct marketing
- **Right to data portability** — to receive your data in a structured, commonly used format and transfer it to another organisation
- **Right to withdraw consent** — where processing is based on your consent (including cookie preferences and newsletter subscription), to withdraw it at any time without affecting the lawfulness of prior processing

To exercise any of these rights, contact us at info@goldphish.com. We will respond within one month of receiving your request. We may need to verify your identity before processing your request.

If you have a concern about how we handle your personal data, we encourage you to contact us first at info@goldphish.com. We will do our best to resolve it promptly and fairly.

If you remain unsatisfied, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). You can contact the ICO at www.ico.org.uk or by calling 0303 123 1113.

---

10. Changes to This Policy

Plain English: *We'll update this policy when our practices change or the law requires it. We'll always update the date at the top so you know when it was last reviewed. For significant changes, we'll take reasonable steps to let you know.*

We may update this Privacy Policy from time to time. The current version will always be available at www.goldphish.com/privacy-policy, with the date of the most recent update shown at the top.

For material changes that affect how we process your personal data, we will take reasonable steps to notify you directly where we hold your contact details.

---

11. Governing Law

Plain English: *This policy is governed by the laws of England and Wales.*

This Privacy Policy is governed by and construed in accordance with the laws of England and Wales. Any disputes arising from this policy shall be subject to the exclusive jurisdiction of the courts of England and Wales.

GOLDPHISH LTD — Company Registration No. 10333752 — ICO Registration No. ZA276913 Registered in England and Wales Goldphish® is a registered trade mark of GOLDPHISH LTD (UK Trade Mark No. UK00003226510) Dalton House, 60 Windsor Avenue, London, SW19 2RR, United Kingdom info@goldphish.com | www.goldphish.com

Last Updated: May 2026