webjects

Data Protection Policy

Webjects Limited — compliance with UK GDPR and the Data Protection Act 2018

COMPANY	Webjects Limited (10521644)
VERSION	1.0
ADOPTED	September 2025
REVIEW CYCLE	Annually — each September
NEXT REVIEW	September 2026
APPROVED BY	Chris Gardner, Director
LEGISLATION	UK GDPR; Data Protection Act 2018; PECR 2003

Webjects · www.webjects.co.uk · Reviewed and approved by Chris Gardner before issue.

PURPOSE

This policy sets out how Webjects Limited ("Webjects", "we", "us") handles personal data, and the standards everyone working for or with us must meet. It explains our duties under the **UK GDPR**, the **Data Protection Act 2018** and the **Privacy and Electronic Communications Regulations 2003 (PECR)** — as amended by the **Data (Use and Access) Act 2025** — and turns those duties into clear, practical commitments.

It serves two audiences: the people whose data we hold — our clients, their site visitors and customers, and anyone who contacts us — and the public-sector bodies, councils, charities and education clients who need assurance that a supplier handles personal data lawfully. It formalises, as a single document we can point to, the privacy position already published on our website.

SCOPE

This policy applies to all personal data Webjects processes, in any format and on any system, and to everyone who processes it on our behalf — the directors, our associates and contractors, and any third party acting under our instructions. **Personal data** means any information relating to an identified or identifiable living individual.

Webjects acts in **two distinct roles**, and the role determines our responsibilities:

· As a **data controller**, we decide why and how personal data is processed — for example, our own client records, enquiries, supplier contacts, marketing lists and staff records. We are registered as a controller with the Information Commissioner's Office (**ICO registration ZA936978**).

· As a **data processor**, we process personal data on a client's behalf and on their instructions — for example, when we host a client's website, manage their database, or run a service that handles their customers' or members' data. Here the client is the controller and we act only within the scope of our agreement with them.

We are a very small company. The commitments below are real and worked into how we operate day to day; they are proportionate to our size and to the nature and volume of the data we handle, as the law allows.

POLICY STATEMENT

> **Webjects is committed to handling all personal data lawfully, fairly, transparently and securely, in full accordance with the UK GDPR, the Data Protection Act 2018 and PECR. We collect only what we need, keep it only as long as we need it, protect it properly, respect individuals' rights, and are honest about what we do with it — whether we are acting as a controller or as a processor for a client.**

We treat data protection as a core part of delivering professional digital services, not an afterthought. We build privacy and security considerations into projects from the outset (data protection by design and by default), and we will not take on processing we cannot carry out safely and lawfully. Where a project involves digital services likely to be used by children, our **Safeguarding Policy** and the ICO's Age-Appropriate Design Code apply alongside this policy.

RESPONSIBILITIES

The Director has overall responsibility for data protection at Webjects and is the point of contact for any data protection question, request or concern: **info@webjects.co.uk**. Given our size, we are not required to appoint a statutory Data Protection Officer and have not done so; the Director carries this responsibility directly.

WHO	RESPONSIBILITY
The Director	Owns this policy; maintains our ICO registration; handles data subject requests, complaints and breaches; approves processor and sub-processor arrangements; reviews this policy annually.
Directors and all personnel	Follow this policy; process personal data only for legitimate, instructed purposes; keep data secure; report any suspected breach to the Director without delay.
Associates and contractors	Process personal data only as instructed and under written terms; apply the same security and confidentiality standards as Webjects staff.

WHAT THIS MEANS IN PRACTICE

The data protection principles (Article 5). When we act as a controller, we apply the seven principles to all personal data. We:

1. process it **lawfully, fairly and transparently** — people know who we are and what we do with their data;
2. collect it only for **specified, explicit and legitimate purposes** and do not reuse it in incompatible ways (**purpose limitation**);
3. limit it to **what is adequate, relevant and necessary** for the purpose (**data minimisation**);
4. keep it **accurate** and up to date, and correct or erase inaccurate data;
5. keep it in identifiable form **no longer than necessary** (**storage limitation**);
6. keep it **secure** against unauthorised access, loss or damage (**integrity and confidentiality**); and
7. take **responsibility** for compliance and are able to demonstrate it (**accountability**).

Lawful basis (Article 6). We identify and document a lawful basis before processing personal data as a controller. In practice this is usually **consent** (e.g. marketing sign-ups), **contract** (e.g. delivering a project a client has engaged us for, or steps taken before a contract), **legal obligation** (e.g. keeping records HMRC requires), or **legitimate interests** (e.g. running and securing our business and

responding to enquiries), having balanced our interests against the individual's rights. We also take account of the **recognised legitimate interests** ground added by the Data (Use and Access) Act 2025 for specific purposes such as safeguarding, crime prevention and responding to emergencies, where it applies. Where we process any special category data, we identify an additional Article 9 condition first.

Individuals' rights and timing. We respect the rights individuals have over their personal data — to be informed; of access (a subject access request); to rectification; to erasure; to restrict or object to processing; to data portability; and rights relating to automated decision-making. We respond to a valid request **without undue delay and within one calendar month** of receiving it. Where we reasonably need more information to identify the person or locate what they have asked for, we may **pause that time limit** until they provide it, in line with the Data (Use and Access) Act 2025. Where a request is complex or we have received several from the same person, we may extend the deadline by up to a further two months and will tell the individual, with reasons, within the first month. Requests are normally free; we may charge a reasonable fee or refuse only where a request is manifestly unfounded or excessive, and we will explain any such decision. When the data we hold belongs to a client (we are the processor), we promptly pass the request to that client and assist them in responding.

Data retention. We keep personal data only as long as we have a genuine need for it, then securely delete or anonymise it. Retention periods are proportionate and documented: for example, we keep financial and tax records for the period HMRC requires (currently at least six years), and we review client and enquiry data periodically and remove what is no longer needed. As a processor, we retain client data only for as long as our agreement requires and return or delete it on the client's instruction at the end of the engagement.

Security of processing (Article 32). We apply appropriate technical and organisational measures to keep personal data secure, proportionate to the risk. These include access controls and strong, unique credentials with multi-factor authentication where available; encryption in transit (HTTPS/TLS) and on devices; reputable, access-controlled hosting; regular software, plugin and security updates on the sites and systems we manage; backups with the ability to restore; and limiting access to those who genuinely need it. We keep client systems patched and monitored as part of our hosting and maintenance services.

Processors and sub-processors (Article 28). Where we engage another organisation to process personal data on our behalf (for example, hosting, email, cloud storage or analytics providers), we use only providers who give sufficient guarantees of compliance, and we put a **written contract** in place containing the terms required by Article 28 — including that the provider acts only on documented instructions, keeps the data confidential and secure, assists with rights requests and breaches, and deletes or returns the data at the end of the service. When **we** act as a processor for a client, we work under the client's Article 28 terms, do not engage a sub-processor without the client's authorisation, and pass equivalent obligations down to any sub-processor we use.

International transfers. We keep personal data in the UK or the European Economic Area wherever practical. Where a transfer is made to a country outside the UK that is not covered by UK 'adequacy' regulations, we put an appropriate safeguard in place before transferring — normally the ICO's

International Data Transfer Agreement (IDTA) or the **UK Addendum** to the EU Standard Contractual Clauses — and carry out a transfer risk assessment where required. Several mainstream tools we use store data outside the UK; we satisfy ourselves that an appropriate transfer mechanism is in place before relying on them.

Cookies and electronic marketing (PECR). On websites we operate, and in advising clients, we follow PECR. We set only strictly necessary cookies without consent; for any non-essential cookies (such as analytics or marketing) we obtain clear, affirmative consent through a cookie banner and explain what each cookie does. For electronic marketing (email, SMS), we rely on consent obtained through unticked opt-in boxes, or the limited 'soft opt-in' to existing customers where its conditions are met, and we include an easy way to unsubscribe in every message.

PERSONAL DATA BREACHES

A **personal data breach** is any security incident that leads to personal data being accidentally or unlawfully destroyed, lost, altered, disclosed or accessed.

1. Anyone who becomes aware of, or suspects, a breach must report it **immediately** to the Director (**info@webjects.co.uk**).
2. We assess and contain it without delay and record it in our internal breach log.
3. If the breach is likely to result in a **risk to people's rights and freedoms**, we notify the **ICO without undue delay and, where feasible, within 72 hours** of becoming aware of it. If we cannot provide all the detail within 72 hours, we report what we have and follow up — letting the ICO know in time matters more than having every fact.
4. If the breach is likely to result in a **high risk** to individuals, we also tell the affected individuals without undue delay, in plain language, with practical steps they can take.
5. Where we are the **processor**, we tell the affected client without undue delay so they can meet their own notification duties.

HOW TO RAISE A CONCERN OR EXERCISE YOUR RIGHTS

Anyone can contact us about how we handle their personal data, make a request to exercise their rights, or raise a concern. Email **info@webjects.co.uk** or write to us at the registered office below. We aim to acknowledge requests and complaints promptly and will always respond within the statutory timescales set out above. In line with the complaint-handling duty introduced by the Data (Use and Access) Act 2025, we acknowledge a data protection complaint and take appropriate steps to respond to it.

You also have the right to complain to the UK supervisory authority, the **Information Commissioner's Office (ICO)**, at any time — though we would welcome the chance to put things right first. The ICO can be reached at **ico.org.uk**, by its helpline on **0303 123 1113**, or at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

CONSEQUENCES OF A BREACH OF THIS POLICY

Following this policy is a condition of working for or with Webjects. A failure to comply may result in disciplinary action for staff, or termination of engagement for associates and contractors, depending on the seriousness. A deliberate or serious misuse of personal data may also be a criminal offence under the Data Protection Act 2018 and may be reported to the relevant authorities. Beyond the personal consequences, breaches can cause real harm to individuals, damage the trust our clients place in us, and expose Webjects to enforcement action and fines from the ICO — which is why we take this seriously.

MONITORING AND REVIEW

The Director monitors compliance with this policy as part of running the business — keeping our ICO registration current, checking processor contracts are in place, and recording any rights requests, complaints and breaches. This is the first version of this policy. We will review it at least **once a year**, and sooner if the law changes, if we adopt a significant new system or service, or following any data protection incident, so that it stays accurate and proportionate to what Webjects actually does.

LEGAL FRAMEWORK

This policy is made under, and should be read alongside, the following UK legislation and guidance:

· **Regulation (EU) 2016/679 as it forms part of UK law (the "UK GDPR")** — the core data protection regime, as amended.

· **Data Protection Act 2018** (legislation.gov.uk/ukpga/2018/12) — the UK statute that sits alongside and supplements the UK GDPR.

· **The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)** (legislation.gov.uk/uksi/2003/2426), as amended — rules on cookies, similar technologies and electronic marketing.

· **Data (Use and Access) Act 2025** (legislation.gov.uk/ukpga/2025/18) — amends the UK GDPR, DPA 2018 and PECR. It updates, but does not replace, the framework above; most of its data protection provisions came into force on 5 February 2026, with the requirement for controllers to operate a complaints-handling procedure commencing later in 2026. We keep our practices aligned with its requirements as they take effect.

Our regulator is the **Information Commissioner's Office (ICO)**, and we follow its guidance, including its guides to the data protection principles, lawful basis, individual rights, security, controller and processor contracts, international transfers, personal data breaches, and PECR (ico.org.uk).

Webjects Limited · Registered office: Unit 24, BSC, The Waterfront, Hood Road, Barry, Vale of Glamorgan, CF62 5QN · Registered in England and Wales, Company No. 10521644 · VAT No. GB 209874576 · ICO registration ZA936978