



Third-Party Data and Hardware Release Policy

Version: 1.0

Effective date: 22 September 2026

Next review: September 2027

This policy sets out a single rule and the reasoning behind it: we release customer data and customer hardware to the verified account holder, and to nobody else. It applies to any request from a person who is not our customer, whatever they claim and whatever they believe they are owed.

1. Why this policy exists

Any hosting provider can expect to be asked, at some point, for something that belongs to a customer rather than to the person doing the asking. A request of that kind might come from a web designer in dispute with a client, from a former employee who wants a copy of a mailbox, from a company that says it has bought a business and wants the servers in our rack released to it, or from somebody who telephones claiming to be the account holder's partner, accountant or solicitor and says the matter is urgent.

Our answer to all of them is no, and we would rather settle that in advance than in the moment. Writing the rule down means our staff apply it the same way every time, and our customers know exactly what stands between their data and somebody else's say-so.

2. What this policy covers

- **Customer data:** website files, databases, mailboxes and their contents, backups, logs, DNS records, domain control, control panel and server credentials, and anything else stored on or passing through our services.
- **Customer hardware:** servers, storage, network equipment and any other property a customer has placed in our racks, together with physical and remote access to it.
- **Account information:** billing records, contact details, support tickets, and the existence of the account itself.

It applies across every service we sell, including shared and reseller hosting, VPS, dedicated servers, colocation, email and Microsoft 365, domains and DNS, and connectivity. It sits alongside our Terms of Service, Privacy Policy, Data Processing Agreement and Acceptable Use and Abuse Policy.

3. The rule

We release the things listed in section 2 to the registered account holder, or to a contact the account holder has named on the account, once we have verified who we are dealing with under section 5. We release them to nobody else.

We do not treat any of the following as authority to release anything, no matter how convincing it looks:

- a claim to own the website, the domain, the design, the code, the data or the equipment;
- an invoice, contract, quotation or unpaid bill between the person asking and our customer;
- a claim to be our customer's employee, former employee, director, business partner, family member, accountant or solicitor;
- an email or telephone call that appears to come from our customer but cannot be verified against the account;
- a letter from a solicitor, a debt collection agency or a trade body, none of which can compel us on its own;
- urgency, commercial pressure, the threat of legal action, or simple persistence.

Whether the person asking is right about the underlying dispute makes no difference to our answer. We are not able to judge who is entitled to a customer's data or equipment, and we will not appoint ourselves the judge of it. That is a matter between our customer and the person asking.

4. The same answer applies to deleting and suspending

A third party cannot have customer data released, and equally cannot have it deleted, suspended, redirected or altered. Complaints about the content of a hosted site are a separate process with a different test, and they are handled under our Acceptable Use and Abuse Policy at abuse@ganderweb.co.uk. That process can result in content being removed. It never results in content being handed to the complainant.

5. How we verify the account holder

Before we act on any instruction that releases data or hardware, we check it against the account. Depending on what is being asked, that means one or more of:

- a ticket raised from inside the client portal, or an email from the address registered on the account;
- passing the account's security checks, which may include two-factor authentication or billing information that only the account holder would hold;
- for anything significant, a call back on the telephone number we already hold, rather than a number supplied in the request itself.

We will not accept a new contact detail that arrives in the same message asking for the release. Where an account's email address or telephone number has changed recently, we verify by a different route before we act. If we cannot satisfy ourselves that we are dealing with the account holder, we do nothing, and we say so.

6. Adding or removing authorised people

Only the account holder can add, change or remove an authorised contact, by a verified instruction under section 5. Nobody can add themselves to an account, and an authorised contact cannot promote themselves or add others. When an authorised contact is removed, their access ends at that point, including access to any hardware access list.

7. Colocated hardware and physical access

- Only people named on the account's access list may enter the data centre space, and they show photographic identification on arrival.
- We do not admit a third-party engineer, contractor or supplier unless our customer has named that person in advance.
- Equipment leaves the building only on a verified written instruction from the account holder, and we record who collected it, what they took and when.
- We do not image, clone, copy or surrender drives or any other storage media to anyone other than the account holder.
- Remote hands work is carried out only on the account holder's instruction, and we will not use that access to extract data for a third party.

An unpaid invoice between our customer and somebody else gives that person no claim over equipment in our racks, and we will not release it to them. Where invoices owed to us are unpaid, what we may do is set out in our Terms of Service and is not affected by this policy.

8. Sale of a business, insolvency and bereavement

Control of an account can pass to someone new, but only on documents, never on assertion. We will act on:

- a verified written instruction from the current account holder transferring the account;

- documentation appointing an administrator, liquidator or trustee over the account holder, after which we take instructions from the appointed officeholder;
- a grant of probate or letters of administration, where the account holder has died;
- an order of a court.

Until one of those is produced and checked, nothing moves. We keep the service running for as long as it is paid for, we release nothing, and we make no changes that would be difficult to undo. Where two parties each claim the same account, we freeze changes to it and tell both of them that we will act on a court order, or on an instruction signed by both, and not before.

9. The one exception: when the law compels us

We are a United Kingdom company, and UK law can require us to disclose data whatever this policy says. We will not pretend otherwise. We will disclose where we are compelled by an order of a court of competent jurisdiction, by a warrant, or by a statutory notice from a public authority that holds the legal power to compel disclosure, including lawful requests handled under the UK GDPR and the Data Protection Act 2018.

Compulsion is not the same as being asked by somebody official-sounding. When a demand arrives, we do all of the following:

- check that the document is genuine, and that the body issuing it holds the power it claims;
- satisfy ourselves that it is in the correct form, taking legal advice where the position is not clear;
- disclose the narrowest set of data the order actually requires, and nothing beyond it;
- record what was disclosed, to whom, and under what authority;
- tell our customer before we disclose, unless the order or the law prohibits us from telling them, in which case we tell them as soon as we are permitted.

An informal request from a police officer or any other authority, made without a warrant, an order or a statutory notice, is not an exception. We will say so politely and ask for the proper instrument. The single case where we may act without one is an immediate risk to a person's life or safety, where we may disclose the minimum necessary to the emergency services and will record and review that decision afterwards.

10. Our suppliers are bound by the same rule

Our data centre partner, registrar partners and other suppliers act as our sub-processors and are bound by obligations equivalent to our own. They are not authorised to release customer data or customer hardware to a third party either. A request made to one of them is referred back to us and answered under this policy. The sub-processors we use are listed in our Data Processing Agreement.

11. What we do when a third party asks

- 1 We record the request: who asked, when, what they wanted, and what they said entitled them to it.
- 2 We refuse it in writing and point the requester at this policy.
- 3 We tell our customer that the request was made, unless the law prevents us from doing so.
- 4 We keep the record, so that a pattern of attempts is visible if one develops.

We also decline to confirm or deny account details to a third party. We will not tell anyone whether a person or business is a customer of ours, what they buy from us, what equipment they hold, or where it sits, because those facts are themselves customer information.

12. If you are the person we have just refused

There is one route that works, and it is quick: ask our customer to contact us themselves. Once they raise a verified request, we will act on it without delay. If you believe you are legally entitled to the data or the equipment and our customer will not cooperate, the remedy is an order from a court, and we will comply with one when it is produced. Asking us again, or asking a different member of our staff, will not produce a different answer.

13. Governing law

This policy is governed by the law of England and Wales and forms part of our Terms of Service. We review it at least annually, and the version and dates at the top of this document show where it stands.

Need this in writing to hand to someone?

We will issue a signed copy of this policy on company letterhead, addressed to the person asking you for the data or the equipment. Email support@ganderweb.co.uk from the address registered on your account.