
Preamble

This document may be augmented or replaced by relevant sections of other parts of our Agreement and should be read in conjunction with other supporting documents, so please check regularly for updates. Please note, by contracting or using any of our services you agree to be bound by all Lantec terms and conditions collectively, which can be viewed in our [Terms of Service](#).

If you have any concerns or queries, please contact us as per our [Support Policy](#).

Contents

1.	Use of Services	1
2.	Acceptable use guidelines	2
3.	Content guidelines	2
4.	Shared Systems	3
5.	Vulnerability Testing	3
6.	Enforcement	4
7.	General	4
8.	Contact Information	5
9.	Privacy policy	5
10.	Disclaimer	5

1. Use of Services

Lantec reserves the right to suspend or cancel Your access to any or all Services provided by Lantec, where Lantec decides that the Service has been inappropriately used. Lantec reserves the right to refuse Services and/or access to its servers to anyone.

Lantec offer hosting space for legitimate content and bandwidth for visitors to access it. All files on a domain must be part of the active website and linked to the site. Sites should not contain any material which does not comply with our content guidelines.

Lantec provides unrestricted, burstable bandwidth on some of the services and for these resources we require that you do not continuously use an unreasonable excess of such resources. Use of them in a temporary, burstable fashion is acceptable.

Lantec offers numbers of mailboxes/aliases with some Product subject to a fair use policy. Mailboxes are intended for direct use by the Product owner and should not be resold or offered for use by third parties without Lantec's prior consent.

Lantec reserve the right to delete mailboxes (including contents) that are deemed inactive and have not been accessed within the last 180 days.

2. Acceptable use guidelines

2.1 You may not use the Services:

in any way that breaches any applicable regulation, UK or International law;

in any way that is fraudulent;

to transmit, or otherwise permit any unsolicited or unauthorised advertising or promotional material or any other form of similar marketing material, also known as SPAM or Unsolicited Commercial email (UCE);

to publish or otherwise distribute Warez, copywritten or other illegal material. The onus is on You to prove that You own the rights to publish material, not for Lantec to prove that You do not;

with IP addresses other than those assigned to you by our staff;

to participate in any nefarious or Service affecting file-sharing/peer-to-peer activities;

to use the server as a Service affecting application server. Using the server to generate large volumes of email from a database is an example of activity that is not allowed. Scripts should not attempt to manipulate the timeouts on servers. These are set at the present values to ensure the reliability of the server. Sites that reset these because they are resource intensive, and thereby adversely affect server performance are not allowed. Scripts that are designed to provide proxy Services, anonymous or otherwise, are not allowed;

to use an excessive amount of server resources. These include bandwidth, processor utilization and / or disk space;

to directly or indirectly cause any of our IP space to be listed in any abuse database / RBL;

to offer HTTP downloads from your site, other than where the files are directly related to the subject matter of the site;

to redirect users from a non-.XXX website to a .XXX top level domain.

3. Content guidelines

These content guidelines apply to any and all services provided by Lantec to You.

3.1 Material published to or transmitted through our servers must:

be accurate (where stating facts);

comply with applicable law in accordance with section xxx of this policy.

3.2 Material must not:

be defamatory of any person;

be obscene, offensive, or inflammatory;

contain any adult material with the exception of content hosted on .XXX domains. Adult material includes all pornography; or otherwise lewd or obscene content. The designation of 'adult material' is left entirely to the discretion of Lantec;

material hosted on .XXX domains must not breach any of the IFFOR policies. These include, but are not limited to:

- .XXX registrants must not display any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, depicting child pornography as defined in the United Nations Convention on the Rights of the child.
- .XXX registrants must agree to permit automated monitoring of their sites by IFFOR or if applicable, any other recognised third party for compliance with IFFOR policies, including without limitation, IFFOR policies requiring site labelling, prohibiting child pornography, and prohibiting content or conduct designed to suggest the presence of child pornography. Registrants must agree not to employ technological or other means to defeat or prevent such monitoring.
- No registrant shall use or permit use of a .XXX domain name for or in connection with email spoofing, phishing, spam, or other forms of malicious behaviour, in accordance with specifications and policies issued by IFFOR from time to time.
- No registrant may register an abusive string in the sTLD including, without limitation, strings that infringe the intellectual property rights of a third party, including common law trademark rights; strings that are obvious variants of well-known trademarks not belonging to the registrant; first and last names of an individual other than the individual or his/her agent or names that suggest the presence of child pornography.

infringe any copyright, or trade mark;

be likely to deceive any person;

promote or assist any illegal activity;

be threatening, abusive or invade another's privacy, or cause annoyance, inconvenience or needless anxiety;

be used to misrepresent your identity or affiliation with any person or organization;

You must moderate and ensure that any end-user submitted content such as forum posts or chat room entries meet with the standards defined within this Policy.

4. Shared Systems

You may not use any shared / community system provided by Lantec in a way that unnecessarily interferes with the normal operation of any shared system, or that consumes a disproportionate fraction of the resources of the system.

For example, we may prohibit the automated or scripted use of a Lantec Mail Service if it has a negative impact on the mail system, or we may require you to repair coding abnormalities in your hosted code if it unnecessarily conflicts with other customer's use of the hosting.

You agree that we may quarantine or delete any data stored on a shared system if the data is infected with malware, or is otherwise corrupted, and has the potential to affect, infect or corrupt the system or other customer's data that is stored on the same system.

5. Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a Lantec system or network, or to breach our security or authentication measures, whether by passive or intrusive techniques without our prior written consent.

6. Enforcement

We will determine, at our discretion, whether there has been a breach of this Acceptable Use Policy by your use of Lantec Services. When a breach of this policy has occurred, we may take such action as we deem appropriate in accordance with section 1 of this Acceptable Use Policy.

Failure to comply with this Acceptable Use Policy constitutes a material breach of our Terms and Conditions upon which you are permitted to use Lantec Services, and may result in our taking all or any of the following actions:

- immediate, temporary or permanent withdrawal of your right to use Lantec Services;
- immediate, temporary or permanent removal or archiving of any content in breach of our Content Standards (as defined in section 3 of this Acceptable Use Policy) uploaded to our servers;
- issue of a warning to you;
- issue of legal proceedings against you for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach;
- further legal action against you;
- disclosure of such information to law enforcement authorities as we reasonably feel is necessary.

We exclude liability for actions taken in response to breaches of this acceptable use policy. The responses described in this policy are not limited, and we may take any other action we reasonably deem appropriate.

We will charge you our standard rates for consequential work on any breach of the AUP together with the cost of any equipment and material needed to:

- investigate or otherwise respond to any suspected violation of this AUP;
- remedy any harm caused to us or any of our customers by the use of your Service in violation of this AUP;
- respond to complaints;
- have our Internet Protocol numbers removed from any abuse database / RBL etc;

7. General

Lantec have a Police Liaison function and we are committed to assisting, and cooperating with, all law enforcement and government agencies in helping to reduce Internet Crime.

We may monitor any content or traffic belonging to you or to users for the purposes of ensuring that the Services are used lawfully. We may intercept or block any content or traffic belonging to you or to users where Services are being used unlawfully or not in accordance with this AUP, and you do not stop or provide us with an acceptable reason within 7 days of receipt of notice from us.

We may, without notice to you:

- report to the appropriate authorities any conduct by you that we believe violates applicable law;
- provide any information we have about you, or your users or your traffic and cooperate in response to a formal or informal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil action that on its face meets the requirements for such a request.

If we are legally required to permit any relevant authority to inspect your content or traffic, you agree that we can, provided however that where possible without breaching any legal or regulatory requirement we give you reasonable prior notice of such requirement and an opportunity to oppose and/or attempt to limit such inspection in each case to the extent reasonably practicable.

8. Contact Information

We are happy to answer any questions You may have regarding Your Lantec Services. Please note that any discussions with Lantec are treated in strictest confidence, and we reserve the right to limit our communication in accordance with our [Support Policy](#).

9. Privacy policy

Your right to privacy is very important. Lantec recognise that when You choose to provide Lantec with information about Yourself, you trust Lantec to act in a responsible manner. We believe this information should only be used to help Lantec provide You with a consistent / improved Service, in accordance with our [Privacy policy](#).

10. Disclaimer

We Lantec and our appointed agents are under no duty, and by this AUP are not deemed to undertake a duty, to monitor or police our customer's activities and we disclaim any responsibility for any abuse or misuse of our network.

Please note: By contracting or using any of our services you agree to be bound by all Lantec terms and conditions collectively, which can be viewed in our [Terms of Service](#).