



We are
Ireland online

Policy Advisory Committee

4 February 2021

Meeting - PAC#26

Policy Advisory Committee - Agenda

1. Membership Matters
2. Minutes from the PAC#25 meeting
3. Matters arising – Registry’s new domain management platform (TITAN)
4. Update on the policy change request relating to the handling of reserved/blocked names
5. Update on the on-going discussion relating to the handling of online abuse
6. Any Other Business
7. Next Meeting

1. Membership Matters

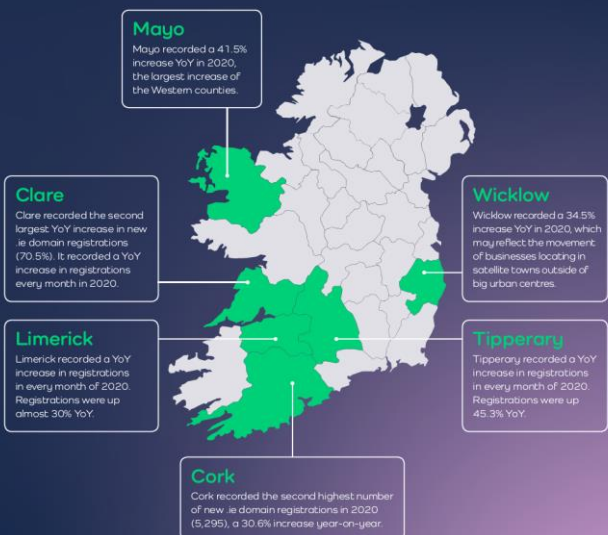
- Please keep **microphones muted** throughout the call
- Please “**raise a hand**” to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
 - Recording will be deleted once the Minutes are approved by PAC

2. Minutes of the PAC #25 Meeting

- Meeting minutes are circulated to the membership within one week of each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on [weare.ie](https://www.weare.ie) after the comment period has ended
- Published online at <https://www.weare.ie/policy-development-process/>

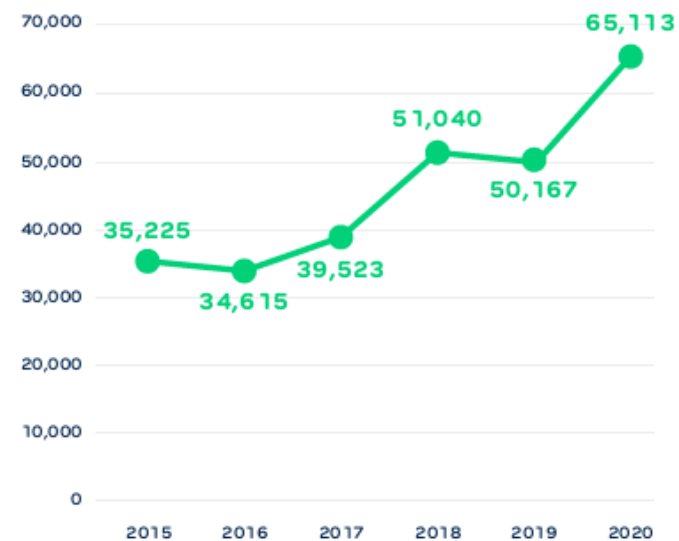
3. Matters arising

Analysis of .ie domains by county



County	Island of Ireland database % share	New registrations 2020	% growth vs 2019
Antrim	0.57%	272	+7.1%
Armagh	0.18%	90	+7.1%
Carlow	1.70%	1,285	+48.0%
Cavan	0.92%	672	+39.1%
Clare	1.82%	1,381	+70.5%
Cork	8.68%	5,295	+30.6%
Derry	0.18%	135	+68.8%
Donegal	1.65%	1,153	+36.8%
Down	0.42%	268	+28.9%
Dublin	44.11%	23,952	+26.3%
Fermanagh	0.06%	43	+34.4%
Galway	4.54%	2,927	+37.8%
Kerry	2.07%	1,422	+31.7%
Kildare	4.50%	2,993	+26.8%
Kilkenny	1.48%	953	+19.3%
Laois	1.01%	733	+13.6%
Leitrim	0.46%	331	+59.9%
Limerick	2.89%	1,714	+29.3%
Longford	0.48%	284	+13.2%
Louth	2.20%	1,364	+25.8%
Mayo	1.77%	1,225	+41.5%
Meath	3.52%	2,373	+34.4%
Monaghan	0.68%	437	+74.1%
Offaly	0.89%	623	+46.2%
Roscommon	0.78%	507	+16.6%
Sligo	1.11%	715	+49.3%
Tipperary	1.77%	1,197	+45.3%
Tyrone	0.20%	129	+63.3%
Waterford	1.85%	1,259	+29.7%
Westmeath	1.30%	861	+29.9%
Wexford	2.52%	1,782	+39.9%
Wicklow	3.69%	2,519	+34.5%
Total	100%	60,894	

NEW REGISTRATIONS



3. Matters arising

Registry's new domain management system (TITAN) – Launched on 16th November

- A platform for the next decade
- Industry standard lifecycle for .ie domains
- Enhanced role and responsibilities for Registrar channel
 - clientHold, exclusive control over edits (Admin Contacts access restricted) etc
- Higher levels of automation (with EPP) and tx speed, with transparency via polling
- Premium CX with TITAN's context-sensitive help function and FAQs, and DeskPro

4. Update on the policy change request relating to the handling of reserved / blocked names

Recap:

- ❖ Discussion topic raised to address the need for enhanced determinism, consistency and clarity
- ❖ A number of potential, **suitable policy responses** were identified
- ❖ Discovery Group was **setup** to review and discuss these options
- ❖ Discovery Group developed **consensus** on a suitable approach
- ❖ Broad consensus established for the identified policy approach
 - which involve making **minor edits** to the “availability” provisions in the Registration & Naming Policy
- ❖ Related policy change request re R&N Policy was submitted at #PAC 23

4. Update on the policy change request relating to the handling of reserved / blocked names

Consensus that an appropriate response should:-

- ❖ be based on the principles of **transparency**, **quality of information** and a **mechanism to “apply”** for a reserved domain name
- ❖ adopt the “EURid (.eu) approach”
 - Address “reserved”/”blocked” names in the “availability” provisions within .ie Registration & Naming Policy
 - **Publish** a non-exhaustive list of ”blocked”/”reserved” names
 - **Publish** user-friendly materials, such as leaflets, with guidance on why/how such names are handled
 - Introduce a defined, transparent **procedure** for facilitating requests to “apply” for “blocked”/”reserved” names

4. Update on the policy change request relating to the handling of reserved / blocked names

Updates:

1. The necessary edits to the Registration and Naming Policy were implemented on **16 November 2020**.
2. .ie domains intended for potential future commercial use by .IE have been reclassified as normal registrations (rather than as blocked/reserved names).
3. User-friendly guidance materials, including helpful on-site content and a leaflet will be published shortly.
4. A web page to provide transparency on blocked/reserved domains will go-live shortly.
5. Wording of a transparent procedure for facilitating requests to “apply” for blocked/reserved names will be published on our website shortly.
6. Appropriate TITAN response messages for lookup requests for blocked/reserved names have been introduced.
7. Policy conclusion - request to be submitted at PAC #27.

Reserved domain names

Request to register Process and procedure



Reserved .ie names

A reserved domain name is one which the Registry has decided to exclude from the list of names available to register. This can occur for a variety of reasons, including commercial considerations, historical, policy or administrative reasons. However, it is possible to apply for a reserved name if you meet certain criteria.

There is also a category of domain names which are blocked for security or technical reasons and these cannot be applied for and will not be available for registration nor will a list of these names be published.

Applying for a .ie reserved name

You may be eligible to apply for a reserved domain name, if you meet the following criteria:

- You can demonstrate a connection to Ireland which is a registration requirement as outlined in the .ie Registration and Naming Policy on www.weare.ie and
- You have legitimate grounds for registering the name, and
- The registration of the name to you is in the public interest of the broader .ie namespace (meaning that the registration of the name to you would represent a substantive benefit to Ireland's internet community).

How to apply for a reserved .ie domain name

To submit a request to register a reserved .ie domain name, all the following information will be required:

- **Domain Name** (including the .ie suffix)
- **Proposed Domain Holder** (who is requesting to register the .ie domain name)
- **Contact Email Address** (this must be an email address for the Domain Holder)
- **Contact Postal Address** (this must be a postal address for the Domain Holder)
- **Contact Phone Number** (this must be a phone number for the Domain Holder)

Supporting information - Include information in support of your request to register this .ie name. Explain why you believe the name should be released from the Reserved Name list, and registered to you. If you are showing your connection to Ireland with a commercial or trademark number, you can include this here.

Email your details to reservednames@weare.ie



What happens next?

1. Our Registration Services Team will review your request.
2. If your request is **accepted**, you'll be asked to contact an accredited .ie Registrar to submit your application. (Note to Registrars: the domain will be reassigned to the eligible domain holder).
3. If your request to register is **refused**, and you feel there is additional information in support of your request that should be taken into consideration, you can provide this information to us using the web form, and we will review the request again.

Our Registration Services Team will review the additional information you provide, and make a recommendation to our Management Team. They will consider your information, along with the recommendation, and either accept or refuse the request.

4. If your request to register is **refused** again, and you feel there is further information that should be taken into consideration, you can submit an appeal to the .IE Board of Directors, by writing to the Company Secretary at our registered address.

The basis for the appeal, together with the supporting information you provide, will then be submitted to the .IE Board of Directors for consideration. The decision of the board will be final.

.ie domain policies

Further information on the full range of .ie domain policies is available on our website www.weare.ie/our-policies

Available .ie domain names

There are many available .ie domain names. You can check for available names on our website www.weare.ie

A .ie domain name is considered to be available if it meets the following conditions. It:

- Must not be currently registered to another party, or
- Must not have any open, pending application requests for registration, or
- Must not be included on the .ie Reserved Name List, or .ie Blocked Name List, as published on our website, www.weare.ie, or
- Must not display a "Reserved" or "Blocked" label on the .ie WHOIS service, or
- Must not be otherwise prohibited from registration by the Registry for technical and/or security reasons. Note that a list of such names is not made publicly available.

Available names can be applied for on a first-come, first-served basis. You can apply through any of our accredited Registrars, listed on our website www.weare.ie/accredited-registrar-list

List of reserved .ie domain names

- dennisjennings.ie
- government.ie
- kid.ie
- pdn.ie
- pin.ie
- porn.ie
- school.ie
- webprofessional.ie
- web-professional.ie
- webprofessionals.ie
- web-professionals.ie

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

Discussion Recap:

The topic was raised for discussion at the PAC#19 meeting:-

- In light of increased concerns of online abuse amongst all internet users
- National / International response focusing on **appropriate, effective, efficient abuse handling**:-
 - EU legislation (e.g. NIS, ENISA, Cybersecurity Act, CPC Regulation), “Notice & Action” etc.
 - Dept. of Communications - recent press release regarding social media and takedown legislation
- to identify the issues involved in developing an appropriate abuse handling strategy
- PAC split discussions into two work streams – **Technical Abuse (5.1)** and **Criminal Abuse (5.2)**

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

Recap..../ continued

- **Stopping abusive activity and removing illegal content**
 - Removal of the content from the Internet is the most *effective* way to avoid content being accessed.
 - Two parties have access to the content (or the device storing it): the **content publisher** and **hosting provider**.
- **What role have ccTLD operators played?**
 - Attempts to “block” abuse at the Registry-level usually result in domain registration **suspension/deletion**
 - Historically, ccTLD operators have taken action as **last resort** (in emergency/Court Order/Law Enforcement)
- **Challenges faced by Registry-level action:-**
 - the abusive content remains **available** (as only the host or content publisher can truly remove it)
 - such measures may have **unintended collateral damage**

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

5.1. Technical abuse

❖ **Discussions** have focused on:-

- how other ccTLDs handle tech abuse
- when action should be taken / who should take it etc.
- the potential introduction of a free informational service for Registrars, such as NetCraft:
 - Alerting Registrars if domains under their management are engaging in abuse
 - Publishing helpful guidelines outlining suggested Registrar action
 - The rationale for this is that Registrars have a direct relationship with the Registrant and/or those managing the registration

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

Recommendation (PAC#24)

.IE and PAC acknowledged:

- increases in registration and technical abuse in other EU ccTLDs
 - ❖ particularly in light of the current Covid-19 situation, and the rise in e-commerce etc.
- need to ensure the **continued safety** of the .ie namespace for the Irish internet community
- intention to progress this work stream to **support the Registrar community** in its response to abuse

Consensus - PAC confirmed to issue a recommendation to the .IE Board for the Registry to:

- introduce a Netcraft-style, free, informational service for Registrars
- publish guidelines for Registrars outlining suggested actions to be taken
(with the Registry working with PAC Registrar reps on word-crafting)

Guidelines for Registrars on handling reported .ie domain technical abuse

The guidelines below have been drafted to assist Registrars in handling reports of technical abuse relating to .ie domains under their management which they receive via the Netcraft reporting service, or otherwise.

The guidelines are not designed to be prescriptive. Registrars may have existing protocols in place, and may take any alternative/additional steps, and provide any advice that they deem appropriate in order to support the registrant in addressing and resolving the reported abusive issue.

If you suspect that a domain is being used in a way which breaches the rules of the .ie namespace, or presents a risk / danger to the .ie DNS or its users, you may use the domain status functionality within the Registry's TITAN systems to temporarily remove the .ie domain in question from the zone whilst you investigate the matter. These domain status features are subject to certain fair use rules, which are detailed [here](#).

Abuse Category	Description	Recommended Action Steps
Malware	<p>Malware refers to software that is used/distributed with malicious intent.</p> <p>It is used by cyber attackers to gain access or cause damage to a computer or network, and/or to gather sensitive/personal information.</p>	<p>We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue.</p> <p>If you are hosting the domain, we recommend that you work with the registrant to clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date.</p> <p>If you are not the hosting provider, we recommend that you help the registrant identify their hosting provider (where possible), and recommend they take the above steps with that party.</p>
Phishing	<p>Phishing is a method of collecting personal information using deceptive e-mails and websites.</p> <p>Phishing messages usually appear to come from well-known organisations. The messages will typically ask a user to click on a link which brings them to a fake site that appears to be legitimate where important</p>	<p>We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue.</p> <p>If you suspect that the domain is being used in connection with illegality, we recommend that you alert the registry.</p> <p>Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps outlined below:</p>

	sensitive/personal information will be requested— such as a credit card number, an account number or a password.	<p>If you are hosting the domain, we recommend that you work with the registrant to correct this matter, remove any incorrect information from the domain and follow best practice for any bulk email marketing on the domain.</p> <p>If you are not the hosting provider, we recommend that you help the registrant identify their hosting provider (where possible), or recommend that they take the steps outlined above with that party.</p>	
Compromised	A compromised domain is one that has been made vulnerable due to unauthorised/third party access. This means that the domain is under the control of a third party.	<p>We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue.</p> <p>If you are hosting the domain, we recommend that you work with the registrant to correct this matter, clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date.</p> <p>If you are not the hosting provider, we recommend that you help the registrant identify their hosting provider (where possible), recommend that they take the steps outlined above with that party.</p>	
Technical Abuse	Technical Abuse is general term that is used to identify an issue. Examples of technical abuse are cryptojacking, ransomware, viruses, hacks and other ever-evolving threats. The issue may be one of the other categories.	<p>We advise that you investigate why the domain use has been reportedly identified as abusive (in a manner that is likely to be considered in breach the rules of the .ie namespace).</p> <p>If you suspect that it has, you may wish to consider suspending the domain using the domain status functionality within TITAN, or alerting the Registry about the party potentially endangering the .ie DNS and/or its users.</p> <p>If you are hosting the domain, we recommend that you work with the registrant to correct this matter, remove any incorrect information from the domain and follow best practice for any bulk email marketing on the domain.</p> <p>If you are not the hosting provider, we recommend that you help the registrant identify their hosting provider (where possible), or recommend that they take the steps outlined above with that party.</p>	
Command and control	This is when a domain is acting as a control centre for a botnet. A botnet is a number of compromised computers running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks and send spam.	<p>We advise that you investigate why the domain use has been reportedly identified as abusive (in a manner that is likely to be considered in breach the rules of the .ie namespace).</p> <p>If you suspect that it has, you may wish to consider suspending the domain using the domain status functionality within TITAN, or alerting the Registry about the party potentially endangering the .ie DNS and/or its users.</p> <p>If you are hosting the domain, we recommend that you work with the registrant to correct this matter, remove any incorrect information from the domain and follow best practice for any bulk email marketing on the domain.</p> <p>If you are not the hosting provider, we recommend that you help the registrant identify their hosting provider (where possible), or recommend that they take the steps outlined above with that party.</p>	
			<p>Spam</p> <p>This domain has been used in connection with the sending of spam or is linked to spam activities.</p> <p>Spam refers to the mass sending of unsolicited emails and may occur in conjunction with phishing or the offering of illegal goods/services.</p> <p>We advise that you check if the domain has been compromised.</p> <p>If you suspect that it has, and that it is being used in connection with technical abuse, such as phishing, we recommend that you follow the steps above, for instances of phishing.</p> <p>If you suspect that the domain is being used in connection with illegality, we recommend that you alert the Registry.</p> <p>Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps as follows:-</p> <p>If you are hosting the domain, we recommend that you work with the registrant to correct the matter, following best practice for any bulk email marketing on the domain.</p> <p>If you are not hosting the domain, we recommend that you help the registrant identify their hosting provider (where possible), recommending that they take the steps outlined above, with that party.</p>

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

Updates and Next Steps

- Helpful guidelines for Registrars are finalised, and were drafted with PAC Registrar representatives input
- These will be circulated to the channel in due course, with 30 days' notice of the planned implementation of the Netcraft service.
- .IE is continuing to work with NetCraft to:-
 - review the practical considerations related to the implementation of the service
 - agree costings / contracting
- Service expected to launch in Q1 2021. Further updates will be provided in due course

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

5.2. Criminal Abuse

- Discussions have focused on potential introduction of a cooperative arrangement with the Garda National Cyber Crime Bureau (GNCCB)
- GNCCB contacted .IE prior to PAC discussion requesting the introduction of such an arrangement
- .IE raised suggestion for PAC input:
 - Some members commented that they felt .IE should be prepared to act responsibly and have a protocol in place to address serious, criminal abuse, if/when it arises.
 - Other members questioned whether there was a genuine need for such an arrangement
- Representatives from GNCCB and Economic Crime Bureau (GNECB) presented at PAC#23 on:
 - what problems they are having with tackling online abuse (particularly with .ie names)
 - which crimes they wish to tackle via a cooperative arrangement
 - what frictions they're experiencing with "normal" channels for suspension/takedown

5. Update on the on-going discussion relating to the handling of abuse in the .ie namespace

5.2. Criminal Abuse

The GNCCB/GNECB representatives also noted that **reactive policing** efforts operate relatively effectively:

- no notable abuse concerns within the .ie namespace
- no notable friction with existing takedown and suspension procedures
- ISPs typically act responsively and responsibly in response to requests from the GNCCB and GNECB

They commented on a shift to **proactive, preventative** policing:

- to combat the tech-savvy nature of criminals (adapting promptly to site takedowns)
- to protect legitimate internet users from becoming victims of serious, life-altering crime

Regarding a potential **Cooperative Arrangement**:

- They acknowledged the important value of a potential arrangement
- Noted that it should be a structured process with appropriate **safeguards** that meet the needs of all stakeholders, and operate in a manner which is mutually beneficial
- Would potentially be used where hosts had failed to address the issue

5. Update on the on-going discussion relating to the handling of online abuse in the .ie namespace

Recommendation (PAC#24)

PAC agreed that there was **consensus**:-

- to re-visit the draft protocol arrangement, and to revise this to ensure the safeguards identified are included
- to circulate this revised edition to the representative from the GNCCB for discussion purposes, and to revert to the PAC with the GNCCB feedback in due course

Updates and Next Steps:

- Edits to the previously drafted protocol arrangement are completed
- The updated template was recently shared with the GNCCB, for discussion purposes
- Further updates will be provided in due course

6. Any Other Business

- 6.1 Policy Conclusion Templates relating to fast-track changes to:
- Registration and Naming Policy
 - Data and Document Retention Policy
 - Privacy Policy
 - WHOIS Policy
- 6.2 Update on industry related developments/legislative changes to be outlined by PAC members
- 6.3 Industry's actions in response to Covid-19 pandemic

6.1 Conclusions of the fast-track policy change requests to:

Policy	Nature of Changes
Registration and Naming Policy	Provisions added relating to the: <ul style="list-style-type: none"> • operation of the new lifecycle (Auto-Renewal and Deletion Processes) and Grace Periods • refunds of the registration fee if a domain is deleted within 14 days of registration • Blocked / reserved names • documentation of the Registry Lock service (this process has been in operation for many years, but not previously added to the Policy) • introduction of new Contact roles/responsibilities for the Registrant • secondary market transactions and domain reassignments – a new Procedure for the Registrant Transfer process will accommodate all requests to change the Registrant granted the right to use a .ie domain. (This will be a single-ticket process to validate new Registrant's 'Connection').
Data and Document Retention Policy	<ul style="list-style-type: none"> • Definitions have been added (this Policy previously hyperlinked to the Privacy Policy definitions) • Clarification provided on the retention of personal data associated with domain contacts (data kept for the lifetime of the contact person, plus two years, provided the contact isn't associated with another .ie domain)
Privacy Policy	<ul style="list-style-type: none"> • Clarification provided on the updated retention practices (as above), and the processing of personal data related to Dispute Resolution services • Clarification provided that personal data may be processed by those providing technical support services in Canada • Edits made to Section 6 on Security and how to update information
WHOIS Services Policy	<ul style="list-style-type: none"> • Expanded to future-proof for RDAP operations • Clarification on field names, including those containing personal data, published via WHOIS Services (continuing to publish the Registrant name where the Registrant is a company or charity (legal person), and redacting the Registrant name for individuals, sole traders etc.) • Clarification on data formats for the Registrar abuse contact role (previously a single, open-text field – but now its a defined contact role)

6. Any Other Business

- 6.1 Policy Conclusion Templates relating to fast-track changes to:
- Registration and Naming Policy
 - Data and Document Retention Policy
 - Privacy Policy
 - WHOIS Policy
- 6.2 Update on industry related developments/legislative changes to be outlined by PAC members
- 6.3 Industry's actions in response to Covid-19 pandemic

7. Next Meeting

Proposed date:

15th April 2021