GAC Advice Response Form for Applicants

The Governmental Advisory Committee (GAC) has issued advice to the ICANN Board of Directors regarding New gTLD applications. Please see Section IV, Annex I, and Annex II of the GAC Beijing Communique for the full list of advice on individual strings, categories of strings, and strings that may warrant further GAC consideration.

Respondents should use this form to ensure their responses are appropriately tracked and routed to the ICANN Board for their consideration. Complete this form and submit it as an attachment to the ICANN Customer Service Center via your CSC Portal with the Subject, "[Application ID] Response to GAC Advice" (for example "1-111-11111 Response to GAC Advice"). All GAC Advice Responses must be received no later than 23:59:59 UTC on 10-May-2013.

Respondent:

Applicant Name	DotKids Foundation Limited
Application ID	1-1309-46695
Applied for TLD (string)	KIDS

Response:

Dear ICANN Board & GAC,

First and foremost, the DotKids Foundation thank the GAC for providing a comprehensive set of advice to the ICANN Board on the subject of safeguards for new gTLDs. We also appreciate the opportunity to provide our response and feedback to the ICANN Board.

As a responsible new gTLD applicant, DotKids Foundation is glad to say that it has already included many measures in the submitted proposal to address the issues raised by the GAC , and believe that its proposal is fully compliant with the GAC advice. We further remain fully prepared to work closely with the GAC and GAC members on any area to further enhance the safeguard measures for the governance and management of the introduction and operations of the .kids gTLD in an orderly, secure and stable manner, technically and socially.

DotKids Foundation understand the critical importance of policies and measures to foster a kids-friendly environment under the .kids gTLD. We especially appreciate GAC's announced principles regarding new gTLDs on March 28, 2007, to respect the provisions of the Universal Declaration of Human Rights and its reaffirmation in the GAC Communiqué – Beijing April 11, 2013.

Today, there are 9 core international human rights treaties focusing on different areas, including Economic, Social and Cultural Rights, Elimination of Racial Discrimination, Elimination of Discrimination against Women, Torture, Rights of Persons with Disabilities and Right of the Child etc. **The United Nations**

Convention on the Rights of Child (UNCRC), is the most widely ratified international human rights treaty[1] which sets out in detail what every child needs to have a safe, happy and fulfilled childhood regardless of their sex, religion, social origin, and where and to whom they were born.

The DotKids Foundation adopts the UNCRC as our guiding principle, with a core mission to run the domain name where we encourage children participation on Internet Governance discussion, and to promote a kids-friendly Internet space, as well as to provide support to the children community, especially to Kids-led initiatives and projects supporting kids' best interests. (for more information about the organizational mission please see main application #18).

The DotKids Foundation application is the only ".kid(s)" application that is in-line with the GAC advice by adopting the UNCRC and is fully respectful of human rights and fundamental freedoms as enshrined in the UN Universal Declaration of Human Rights where the UN has proclaimed that childhood is entitled to special care and assistance.

The DotKids initiative has received support from over 50 children's welfare and rights organizations around the world. Among which UNICEF[2], Save the Children[3], Boys' and Girls' Club[4] are already signed supporters of the DotKids initiative.

As a participant in the ICANN process, we are encouraged by the active participation of the GAC in the process. The GAC and governments are an important component of the ICANN process and the multi-stakeholder governance of the Internet's root DNS. Many of the issues raised by the GAC advice are issues that are actively discussed by the ICANN community. Some of which are already included in the considerations for this round of new gTLDs, some others are currently being discussed within the ICANN process. For example, policy development processes for WHOIS are ongoing and registration and usage abuse issues continue to be examined, including especially where such abuse issues should be within or beyond the scope of ICANN's purview.

For such items, we understand that ongoing multi-stakeholder processes should not be circumvented, and remain diligent against such undermining. Nevertheless, we are fully prepared to improve on our proposed mechanisms in our application as

[1] UNCRC has been ratified by the most countries among all of the Convention than any other human rights treaty in history whereby 192 countries had become State Parties to the Convention as of November 2005. Only two countries, Somalia and the United States, have not yet ratified this celebrated agreement. Somalia is currently unable to proceed to ratification as it has no recognized government. By signing the Convention, the United States has signalled its intention to ratify. (Reference Link: http://www.unicef.org/crc/index_30229.html)
[2] Hong Kong Committee for UNICEF
[3] Save the Children Hong Kong
[4] The Boys' and Girls' Clubs Association of Hong Kong

well as to implement appropriate measures for.kids specifically as Registry policies before community wide ICANN policies are fully in place.

Most importantly, as we applaud the GAC on raising the issues and echo the recommendations to the ICANN Board, we especially suggest that the ICANN Board take care in considering changes made by applicants at this stage in this round of new gTLDs. We believe that the ICANN board should place some weight on considering the approval (and/or dismissal for that matter) of applications where substantive changes to proposed policies for governing and/or operating the gTLD are made as reactionary measures rather than as originally proposed.

The integrity of ICANN and the new gTLD process is at stake. Where appropriate and especially where having a choice, ICANN should approve applications that demonstrate their integrity in standing by their proposal as originally submitted and willingness to participate and respect the ICANN multi-stakeholder bottom-up process, including advice from the ACs. For example, DotKids Foundation's proposal for the .kids registry already adopts the UNCRC and has incorporated many different policies to comprehensively address the GAC advice while other applications for .kid(s) did not.

Finally, we also bring your attention to the ongoing work underway since the recent CEO Roundtables and further discussed at the DNS Summit (http://blog.icann.org/2013/04/dns-summit-in-new-york/). Especially the "proposals to codify ethical standards for DNS businesses", which may be an appropriate framework for addressing issues (e.g. content related) that may be beyond the scope of ICANN's policy mandate.

Attached further are specific responses to each of the issues raised in the GAC advice with excerpts from particular sections of the submitted DotKids Foundation proposal (https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails:downloadapplication/161?t:ac=161) and how it complies with and relates to the GAC advice.

We look forward to continuing the dialogue with the ICANN board and the GAC to address issues and put policies in place to mitigate against concerns in a constructive and prompt manner.

Sincerely,

DotKids Foundation

GAC Advice Response Form for Applicants

DotKids Foundation Response to GAC Communiqué – Beijing April 11, 2013

b. Safeguard Advice for New gTLDs To reinforce existing processes for raising and addressing concerns the GAC is providing safeguard advice to apply to broad categories of strings (see Annex I).

Please see response for Annex I further below.

e. Community Support for Applications The GAC advises the Board: i. that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information.

We are supportive of this advice, especially for the positive impact to an impacted community should an appropriate community application be approved and selected to operate the new gTLD. The original provisions in the Applicant Guidebook (AGB) while provided a scoring system for community priority evaluation (CPE) was predicated on a concern for mitigating against abusive community designation given the priority of delegation if an application has satisfied the criteria of a community. Given that we have now already received all the applications for this round of new gTLDs and community designation responses, the ICANN Board (and staff) should be able to much better fine tune CPE scoring and evaluation, especially in response to this GAC advice. We therefore sincerely urge the ICANN Board to constructively provide further guidelines to evaluators to better support "that in those cases where a community, which is clearly impacted by a set of new gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinion should be duly taken into account, together with all other relevant information."

The ".kid(s)" gTLD clearly targets children. Applicants for ".kid(s)" who do not adopt the United Nations Convention on the Rights of the Child (UNCRC) as their guiding principle represents an imminent potential harm to the kids community around the world.

DotKids Foundation, is the only Community TLD Applicant for the ".kid(s)" string and is the only applicant that adopts the UNCRC. We have been in dialogue with the child welfare and child rights community and understand that they share the concern and has a strong view that ".kid(s)" gTLD must adopt the principles of "UNCRC" in order to avoid and mitigate any potential harm to the community. There are many organisations dedicated to the kids community. Major international ones include UNICEF, Save the Children, Free the Children, Big Brothers Big Sisters,

Boys & Girls Club and many more. Among which UNICEF[5], Save the Children[6], Boys' and Girls' Club[7] and over 50 other children's rights, children's welfare and children-led organizations around the world are already signed supporters of the DotKids initiative.

g. Protections for Intergovernmental Organisations The GAC stresses that the IGOs perform an important global public mission with public funds, they are the creations of government under international law, and their names and acronyms warrant special protection in an expanded DNS. Such protection, which the GAC has previously advised, should be a priority. This recognizes that IGOs are in an objectively different category to other rights holders, warranting special protection by ICANN in the DNS, while also preserving sufficient flexibility for workable implementation. The GAC is mindful of outstanding implementation issues and commits to actively working with IGOs, the Board, and ICANN Staff to find a workable and timely way forward. Pending the resolution of these implementation issues, the GAC reiterates its advice to the ICANN Board that: i. appropriate preventative initial protection for the IGO names and acronyms on the provided list be in place before any new gTLDs would launch.

We are supportive of this advice as a preventative initial protection for the IGO names and acronyms.

In our original submission for #22, we have already included the following in our proposal:

More specifically, the Registry commits to:

a) Adopt, before the new gTLD is introduced, appropriate procedures for blocking, at no cost and upon demand of governments, public authorities or IGOs, names with national or geographic significance at the second level of the TLD.

b) Ensure procedures to allow governments, public authorities or IGOs to challenge abuses of names with national or geographic significance at the second level of the TLD

Building on the experience from .INFO and .ASIA in their handling of country and government related names, the Registry will develop and establish policies for:

1) obtaining and maintaining a list of names with national or geographic significance to be reserved (at no cost to governments) upon the demand of governments, public authorities or IGOs;

[5] Hong Kong Committee for UNICEF
[6] Save the Children Hong Kong
[7] The Boys' and Girls' Clubs Association of Hong Kong

2) process for registrants to apply for and for the Registry to obtain consent from the respective government, public authorities or IGOs in the releasing of such reserved geographic names; and

The procedures may be similar to the management of governmental reserved names for .ASIA (Section 3.4 of http://dot.asia/policies/DotAsia-Reserved-Names--COMPLETE-2007-08-10.pdf). In summary:

I) The Registry will adhere to the New gTLD Registry Agreement Specification 5 requirements regarding 2. Two-Character Labels as well as 5. Country and Territory Names;

II) Before the launch of the TLD, the Registry will also proactively reach out to governments around the world, especially through GAC members (and ccTLD managers where appropriate), to solicit from them their demand for reserving any names with national or geographic significance at the second level of the TLD;

III) The Registry will develop mechanisms and maintain a list of governmental reference contacts, especially through correspondence with GAC members and ccTLD managers where appropriate. The corresponding reference contact(s) will be contacted in case a registration request is received for a governmental reserved name. If the consent from the governmental contact is received, the registration request will be approved. The domain will nevertheless remain in the reserved names list so that in case the registration lapses, the domain will not be released into the available pool, but will require the same approval process to be registered.

IV) The Registry will maintain an ongoing process for adding and updating governmental reserved names as they are demanded by governments, public authorities or IGOs.

In accordance with Specification 5 of the New gTLD Registry Agreement, the registry operator must initially reserve all geographic names at the second level, and at all other levels within the TLD at which the registry operator provides for registrations.

…

Furthermore, the Registry will actively participate in the development of appropriate process and policies for governments, public authorities or IGOs to challenge abuses of names with national or geographic significance. As an important stakeholder in the Registry, DotAsia Organisation (through Namesphere) will be supporting the efforts as well. DotAsia has been a pioneer of protective measures for new gTLDs, especially in its handling of governmental reserved names and its engagement with different stakeholders to develop rapid suspension policies, which provided part of the genesis of what is now standardized for new gTLDs as the URS (Uniform Rapid Suspension) process. Similar administrative processes may be explored and developed for

supporting challenge processes for abuses of names with national or geographic significance.

The above mechanism can be used for the protection of IGO names.

2. Registrar Accreditation Agreement (RAA)
Consistent with previous communications to the ICANN Board
a. the GAC advises the ICANN Board that:
i. the 2013 Registrar Accreditation Agreement should be finalized before any new gTLD contracts are approved.
The GAC also strongly supports the amendment to the new gTLD registry agreement that would require new gTLD registry operators to use only those registrars that have signed the 2013 RAA. The GAC appreciates the improvements to the RAA that incorporate the 2009 GAC---Law Enforcement Recommendations. The GAC is also pleased with the progress on providing verification and improving accuracy of registrant data and supports continuing efforts to identify preventative mechanisms that help deter criminal or other illegal activity. Furthermore the GAC urges all stakeholders to accelerate the implementation of accreditation programs for privacy and proxy services for WHOIS.

We are supportive of the direction of this advice to promote registrant rights and the provisioning of accurate WHOIS data. We further prompt the ICANN Board to realize that within the current ICANN gTLD Registry-Registrar framework, WHOIS (i.e. contact) data is obtained by and remains within the purview of Registrars and not the Registry. In order for the Registry to effectively take action, Registrar compliance will be crucial.

Further discussions included in response to Annex I, point 1. below.

3. WHOIS
The GAC urges the ICANN Board to:
a. ensure that the GAC Principles Regarding gTLD WHOIS Services, approved in 2007, are duly taken into account by the recently established Directory Services Expert Working Group. The GAC stands ready to respond to any questions with regard to the GAC Principles. The GAC also expects its views to be incorporated into whatever subsequent policy development process might be initiated once the Expert Working Group concludes its efforts.

We are supportive of this advice and agrees that matters pertaining WHOIS should best be considered and discussed through the ongoing policy development process on the matter.

4. International Olympic Committee and Red Cross /Red Crescent
Consistent with its previous communications, the GAC advises the ICANN Board to:

a. amend the provisions in the new gTLD Registry Agreement pertaining to the IOC/RCRC names to confirm that the protections will be made permanent prior to the delegation of any new gTLDs.

We are prepared to implement such protections. Based on our original submission, and as explained above in "g. Protections for Intergovernmental Organisations", this can be addressed within the proposed mechanism.

5. Public Interest Commitments Specifications The GAC requests: b. more information on the Public Interest Commitments Specifications on the basis of the questions listed in annex II.

We are prepared to adhere and abide by our Public Interest Commitments including policy proposals submitted within our original proposal as well as our PIC submission: https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails:downloadpicposting/161?t:ac=161

Annex I Safeguards on New gTLDs The GAC considers that Safeguards should apply to broad categories of strings. For clarity, this means any application for a relevant string in the current or future rounds, in all languages applied for. The GAC advises the Board that all safeguards highlighted in this document as well as any other safeguard requested by the ICANN Board and/or implemented by the new gTLD registry and registrars should: • be implemented in a manner that is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights. • respect all substantive and procedural laws under the applicable jurisdictions. • be operated in an open manner consistent with general principles of openness and non-discrimination.

DotKids Foundation is committed to governing and operating the Registry in a manner that

- is fully respectful of human rights and fundamental freedoms as enshrined in international and, as appropriate, regional declarations, conventions, treaties and other legal instruments – including, but not limited to, the UN Universal Declaration of Human Rights.

- respect all substantive and procedural laws under the applicable jurisdictions.
- be operated in an open manner consistent with general principles of openness and non-discrimination.

Under the UN Universal Declaration of Human Rights, there are 9 core international human rights treaties focusing on different areas, including Economic, Social and Cultural Rights, Elimination of Racial Discrimination, Elimination of Discrimination against Women, Torture, Rights of Persons with Disabilities and Right of the Child, etc. The United Nations Convention on the Rights of Child (UNCRC), is the most widely ratified international human rights treaty which sets out in detail what every child needs to have a safe, happy and fulfilled childhood regardless of their sex, religion, social origin, and where and to whom they were born.

Referring to the Application Section 18(a)(a) and 20(e), "*the Registry Operator makes a commitment to adopt the United Nations Convention on the Rights of the Child (UNCRC) as a fundamental guiding principle.*"

Furthermore:

- Referring to the Application #18(a)(b) and 20(c), "*the Registry Operator makes a commitment to support and encourage children's participation in Internet governance by making the governance of the .kids TLD itself a platform for children to participate as an important stakeholder in the multi-stakeholder approach.*"

- Referring to the Application #18(a)(c) and 20(e), "*the Registry Operator makes a commitment to promote kids-friendly content on the Internet with relevant registration policies and guidelines for the registrants based on the UNCRC.*"

- Referring to the Application #18(a)(d), "*the Registry Operator makes a commitment to contribute to the children community including supporting children's rights organizations and initiatives, especially with relevance to the development of the Internet in the best interests of the child.*"

These measures relate to the UNCRC articles for children participation, protection and welfare:

According to Article 17 of the UNCRC, it encourages the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

According to UNCRC Article 13, the child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information

and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

According to UNCRC Article Article 12, the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

On issues of "respect all substantive and procedural laws under the applicable jurisdictions":

- Referring to the Application #28, "*the Registry Operator is prepared to call upon relevant law enforcement bodies as needed. The specific action is dependent upon the jurisdiction of which the registry operator, but the operator in all cases will adhere to applicable laws and regulations. When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Our backend registry provider, Afilias sets a goal to respond to such requests within 24 hours.*"

- Referring to the Application #29.3.3, "*the Registry Operator has already accounted for the compliance of national law not only by our registry, but also on our partners (Front-End Services Provider and Back-End Services Provider) via the binding Registry-Registrar and Registrar-Registrant Agreements… Registrants to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry.*"

On issues of the Registry to be operated in an "open manner consistent with general principles of openness and non-discrimination":

Referring to 20 (c)(c), "*the Registry Operator's vision is rooted in the UNCRC and accepts the guiding principles of the Convention, including non-discrimination; adherence to the best interests of the child; the right to survival, protection and development; and the right to participation by the child. The Declaration already outlines the guidelines on openness and non-discrimination especially to a more vulnerable group of users on the Internet, children.*"

- Referring to #29, provisions in our proposal for additional Rights Protection Mechanisms to provide a strong balance for users' rights beyond just providing protection to Intellectual Property rights: *"Furthermore, on top of the Sunrise program, a Pioneer Domains Program will be put in place to provide even further protection for prior rights holders while maintaining a strong balance against users' rights."*

Safeguards Applicable to all New gTLDs
The GAC Advises that the following six safeguards should apply to all new gTLDs and be subject to contractual oversight.

We are prepared to be subjected to contractual oversight for safeguards applicable to all new gTLDs.

1. WHOIS verification and checks — Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

We are supportive of the direction for this advice and believe that we are already compliant. The scope and specific standard implementation of such policies may best be developed as a product of the ongoing WHOIS policy development process.

Nevertheless, individual Registry policies can provide the interim solution for this safeguard, and some of the mechanisms have already been provided in our original response to #28 Abuse Prevention and Mitigation:

Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

WHOIS data accuracy

The registry operator will offer a "thick" registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as

defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http://wdprs.internic.net/).

The above are the baseline abuse prevention and mitigation measures of the registry. The registry is prepared to work with ICANN and the GAC to further enhance the measures where appropriate.

2. Mitigating abusive activity — Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

We are prepared to and have already proposed to include in our Registry-Registrar Agreement (RRA) provisions to ensure that terms of use for registrants include prohibitions against abusive activities.

The following is an extract from our response to #28 Abuse Prevention and Mitigation:

Anti-Abuse Policy
The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:
• Illegal or fraudulent actions;
• Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
• Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
• Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
• Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
• Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
• Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
• Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity

that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Furthermore,

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

3. Security checks — While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

We are supportive of proactive measures to ensure the security and stability of the Internet. As indicated in the GAC advice, the respecting of privacy and confidentiality is paramount. Furthermore, while the inclusion of appropriate terms of use for registrants as described in "2. Mitigating abusive activity" above provides an effective enforcement mechanism, the subject matter of certain threats may traverse beyond the purview of ICANN policy coordination. For example matters concerning content. Such determination may best be addressed in proper ICANN policy development processes if implemented as a contractual and enforcement matter by ICANN.

Nevertheless, the Registry is fully prepared to implement policies within the registry and have already proposed such mechanisms in our original application under #28 Abuse Prevention and Mitigation:

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.

b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
• Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
• The identity of a proxy-protected registrant;
• The purchaser's IP address;
• Whether there is a reseller involved, and;
• The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
- *Registration information*
- *History of a domain, including recent updates made*
- *Other domains associated with a registrant's account*
- *Patterns of registrant portfolio*

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
- *Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.*
- *Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.*
- *Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]*

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

4. Documentation — Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

We are supportive of the conceptual directive and are prepared to maintain such documentation. We however caution about misinterpretation and/or misuse of such statistical data.

As proposed in our application (under #28 Abuse Prevention and Mitigation):

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:

• *Number of abuse reports received by the registry's abuse point of contact described above;*
• *Number of cases and domains referred to registrars for resolution;*
• *Number of cases and domains where the registry took direct action;*
• *Resolution times;*
• *Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;*
• *Phishing site uptimes in the TLD.*

…

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

5. Making and Handling Complaints – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

We are supportive of this advice ad believe that our original proposal is already compliant with the GAC advice. Description of the mechanisms for handling complaints have been included in our response to #28 Abuse Prevention and Mitigation:

Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.kids". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based

approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

In addition, DotKids will also feature a complaint platform for users on the Internet to file complaints for potentially abusive domains under .kids (#20e):

Open Compliant Platform and Immediate Process

Every netizen can file a complaint via the online portal with clear indication of the point of inappropriate content. The online portal enables all Internet users to contribute on building a kids-friendly Internet space at ease.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

6. Consequences – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

We are supportive of including mechanisms to suspend a domain name against abusive activities and believe we are already compliant with the GAC advice. In our proposal (under #28 Abuse Prevention and Mitigation and #29 Rights Protection Mechanisms), we have already included mechanisms to disqualify, suspend, cancel or delete domain registrations where appropriate:

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any

applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

In enforcing the special community requirements for the ".kids" TLD (#20e):

The DotKids Foundation has developed a set of Guiding Principles as described above in A) and will continue to refine such Guiding Principles under the guidance of the community. It is mandatory for all .kids registrants to adhere to the Guiding Principles. Violation of the principles, whether or not intentionally by the registrant, especially if such violation results in the proliferation of materials likely to harm and disturb kids, will be grounds for cancelation, suspension and takedown of the domain name.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

Category 1 Consumer Protection, Sensitive Strings, and Regulated Markets:
The GAC Advises the ICANN Board:
• Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. The following safeguards should apply to strings that are related to these sectors:

1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

We are prepared to be and believe that our proposal is already compliant with this advice.

As part of our response to #28 Abuse Prevention and Mitigation, we have included provisions to ensure that registrants comply with all applicable laws:

The registry operator definition of abusive use of a domain includes, without limitation, the following:
• *Illegal or fraudulent actions;*

- *Spam;*
- *Phishing;*
- *Pharming;*
- *Willful distribution of malware;*
- *Malicious fast-flux hosting;*
- *Botnet command and control;*
- *Illegal Access to Other Computers or Networks.*

Furthermore, in response to #18c Rules to minimize social costs and #20e Registration policies, we have outlined additional policies and mechanisms to safeguard against consumer harm:

4. Protection Scheme

To facilitate the enforcement of the Guiding Principles described in 20e A. Eligibility, an express complaint-response system will be implemented through an online portal. The online portal will accept complaint reports of any inappropriate content from the public through a structured report form (i.e. such that the complainant can indicate the type of inappropriate content they are reporting and its severity in the view of the complainant, etc.). Upon the receipt of a complaint report, a takedown decision process will be initiated depending on the type of complaint report filed:

1: Illegal Content & Activities

In the case of a complaint report filed alleging illegal content and activity, the Registry, with the support from Afilias as the registry back-end services provider, will activate the Anti-Abuse process as described in #28 (Abuse Prevention & Mitigation). If the investigation based on the Abuse Policy finds the complaint to be substantiated, the Registry, with the support from Afilias, will act according to the Abuse Policy. If the investigation finds the complaint not to be of an abusive nature in the view of the Abuse Policy, the complaint will be passed to 2.

2: Inappropriate Content

In the case of a complaint report filed alleging inappropriate content or activity (or as a result of 1 above), the complaint report will be passed to the Monitoring Committee for further process. Anyone online can access the complaint-response portal to file a complaint report. This includes the DotKids Foundation itself as well as all members of the Foundation and members of the community. In fact, the DotKids Foundation is prepared to proactively guard against inappropriate content through this mechanism. A complaint report should clearly state the rationale of why the content or activity should be considered inappropriate and how the .kids domain is inconsistent with the .kids Guiding Principles and should be suspended.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.

We are prepared to be and believe our proposal is compliant with this advice. The Registry will specify in its Registry-Registrar Agreement (RRA) that all registrants must be notified of this requirement at the time of registration.

3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.

We are prepared to be and believe that our proposal is already compliant with this advice. As described in 1. above, illegal behaviour under applicable law is considered abusive activities disallowed by the registry. The Registry will have the ability to utilize the APM (Abuse Prevention & Mitigation) mechanisms to suspend, cancel, delete or otherwise take action against the domain registration.

In addition, as stated in our application question #18 and #20(e), DotKids Foundation adopts the United Nations Convention on the Rights of the Child (UNCRC) as the fundamental guiding principles. Appropriate guidelines will be developed by the community members of DotKids Foundation for registrants to create kids-friendly website based on the UNCRC principles.

According to the Article 16 of UNCRC, which states that the following:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.

in other words, children have the right to protection of their privacy and thus DotKids Foundation is committed to develop relevant policies and the kids-friendly guidelines mentioned above in accordance to these principles.

In view of the special needs of kids, a Protection Mechanism will be in place. We have designed an online portal where any Internet users can report any harmful contents or misconduct of the registrants via their domains to the kids. A Monitoring Committee formed by children experts from around the globe will then be allowed to vote on whether the content is harmful and its level of severity so as to carry out the further necessary actions such as suspension or take-down of the domain. Moreover, serious offences of the content guideline or any illegal activities will be handled immediately. Details of the Protection Mechanism and the enforcement could be found in question 20(e) of our application.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

4. Establish a working relationship with the relevant regulatory, or industry self--- regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

We are supportive of, fully prepared to be and believe our proposal is already compliant with this advice.

As stated in the earlier part and also in our application #20(b), DotKids Foundation will be formed as a membership consortium of the children-rights organizations and child-led group worldwide whereby the community will be the backbone of the governance structure and form the board of councillors and respective advisory councils. The high level engagement of the community members in the policy development process will help to devise strategy in mitigating as much as possible the risks of fraudulent, illegal and other activities that are detrimental to the kids community with references to the universal principles and standards among the community, i.e. the United Nations Convention on the Rights of the Child (UNCRC).

The DotKids Foundation has already reached out to and is establishing a working relationship with many relevant industry bodies and associations:

International Regulatory Bodies:
The United Nations Committee on the Convention on the Rights of the Child (CRC Committee)

Child-right Alliances:
- EuroChild, Brussels
- European NGO Alliance for Child Safety Online (eNACSO)
- Child Rights Coalition Asia (CRC Asia)

International and local child-centric organizations:
- UNICEF International
- Save the Children
- NetSafe, New Zealand
- INHOPE, Ambsterdam

In our submitted application and also the continuous outreach work, we have already established a relationship with and obtained the support from many different organizations:

<u>Moldova</u>
Child Rights Information Center Moldova

<u>Russia</u>

The Foundation for Network Initiatives "The Smart Internet"

Australia
Mr. Alasdair Roy
Children and Young People Commissioner
ACT Human Rights Commission, Canberra Australia

Norway
Mr. Reidar Hjermann
Former ombudsman for children in Norway, Clinical psychologist,
Expert in human rights and participation for children and young people

China/ Hong Kong
Hong Kong Youth Synergy
Internet Learning Support Centre
NetMission.Asia
The Hong Kong Academy for Gifted Education
Mr. Dennis Chi Kuen Ho
Alliance for Children's Commission
Against Child Abuse
Baby Friendly Hospital Initiative Hong Kong Association
Caritas Family Crisis Line & Education Centre, Children Counseling Services
Caritas Youth and Community Service
Children Rights Association
Chinese YMCA of Hong Kong – Hin Keng Centre
Evangelical Lutheran Church of Hong Kong Social Service Head Office
The Hong Kong Childhood Injury Prevention and Research Association
Hong Kong College of Paediatricians
Hong Kong Committee for UNICEF
Hong Kong Committee on Children's Rights
Hong Kong Council of Early Childhood Education and Services
Hong Kong Down Syndrome Association
Hong Kong Society for the Protection of Children
Kids' Dream
Playright Children' s Play Association
Save the Children Hong Kong
Society for Community Organization
Suen Mei Speech & Hearing Centre
The Boys' and Girls' Clubs Association of Hong Kong
The Hong Kong Council of Social Service
TREATS
Ms Chan C.Y. Eliza
Mr Ken Chan
Dr Cheung Chiu Hung, Fernando
Dr Kwok Ka Ki
Mrs Priscilla Lui

Mrs Mak Yau Mei Siu, Teresa

Asia Region
Child Rights Coalition Asia (CRC Asia)
Cambodia NGO Committee on the Rights of the Child (NGOCRC)

China/ Hong Kong
Hong Kong Committee on Children's Rights (HKCCR)

Indonesia
Children's Human Rights Foundation
Yayasan SEJIWA
Yayasan KKSP – Education and Information Centre for Child Rights
Sahabat Perempuan dan Anak Indonesia (SAPA Indonesia)

Philippines
Mindanao Action Group for Children's Rights and Protection (MAG-CRP)

Malaysia
Protect and Save the Children – Malaysia

Myanmar
Human Rights Education Institute of Burma (HREIB)
United Against Child Trafficking (United ACT)

Thailand
The Life Skills Development Foundation (TLSDF)

Vietnam
Vietnam Association for the Protection of Children's Rights (VAPCR)
Centre for Research and Support for Vietnamese Children (CENFORCHIL)
Paradise for Children Network (PCNet)
Institute for Social Studies (ISS)

Regional
Southeast Asia Coalition to Stop the Use of Child Soldiers (SEASUCS)
Save the Children Sweden – Southeast Asia and Pacific Regional Office
Terre des Hommes Germany in Southeast Asia
NGO Advisory Council for the Follow-up of the UN Secretary-General's Study on Violence Against Children

Furthermore, the DotKids Foundation is formed as a consortium of industry organizations and committed to continued outreach to relevant industry regulatory bodies:

About DotKids Foundation

The operating registry, DotKids Foundation, is a not-for-profit organization founded with the support of children rights organizations and a governance structure that openly invites children as well as children's rights organizations to participate in the application and operation of the domain ".kids".

…the Foundation and actively reach out to the community and invite children-right organizations to join the Foundation as members and form the Board of Councilors and Advisory Councils according to the following framework.

Special Features of the Governance Structure and Operation:
1. A membership consortium formed by children-right organizations and children-led groups
2. Board Members formed by children-right organizations and professional individuals
3. Advisory Councils formed by children right professionals, IT technology specialist and children-led groups

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

We are supportive of the conceptual direction of this advice to be able to connect with registrants in a timely fashion. At the same time, we also understand that within the current ICANN gTLD Registry-Registrar framework, the Registry should rely on the Sponsoring Registrar to connect with registrants. Many Registrars feel that it is inappropriate for the Registry to directly contacting the registrant.

Nevertheless, in balancing the above considerations, it is possible to setup an "Operations and Notifications Contact" (for example, this was approach was successfully implemented to address similar conditions during the original .ASIA ASCII launch), which Registrars and/or registrants may select to nominate, with default being either the Registrar contact or the Admin Contact for the registrant.

We are prepared to explore to include additional safeguards where appropriate in consultation with ICANN and the GAC.

The GAC further advises the Board:

1. In addition, some of the above strings may require further targeted safeguards, to address specific risks, and to bring registry policies in line with arrangements in place offline. In particular, a limited subset of the above strings are associated with

market sectors which have clear and/or regulated entry requirements (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) in multiple jurisdictions, and the additional safeguards below should apply to some of the strings in those sectors:

6. At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.

Credentials of registrants will be checked with the Registrant pre-verification and authentication process as part of the Abuse prevention and mitigation mechanisms (#28):

Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

- *Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.*
- *Based on required WHOIS Data; registrant contact details (name, address, phone)*
- *If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)*
- *If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.*
- *If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.*
- *If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.*
- *WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".*

• *A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would show limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.*
• *Validation would be annually renewed, and validation date displayed in the WHOIS.*

Eligibility of Registrants are verified and subject to challenge during startup phases including Sunrise (#29 Rights Protection Mechanisms):

29.1.3 Sunrise Challenge (Dispute Resolution) Process

Besides a contention resolution process, an important part of any Sunrise process is a well developed Sunrise Challenge Process to ensure the integrity of the Sunrise program. The Sunrise Challenge Process is important such that after the allocation of a Sunrise name, there is a period of time where legitimate rights owners can challenge the legitimacy and eligibility of a registrant based on the Sunrise policies to a domain name.

Furthermore, in response to #20e Registration policies, we have outlined additional policies and mechanisms to safeguard against consumer harm based on the eligibility of registrants:

A) Eligibility: For registering a second-level name, and how will eligibility be determined

The .kids TLD is restricted to children centric organizations, non-governmental organizations (NGOs), children's rights initiatives and children led initiatives in the first phase of Sunrise. A multi-phased Sunrise process will be adopted (for more information please see application form #29).

In a subsequent Sunrise phase, the standard ICANN new gTLD sunrise and Trademark Clearing House implementation will be offered for legitimate registered trademarks and service marks owners to obtain domains corresponding to their entity names.

Throughout the Sunrise, Landrush phases and upon Go Live, the .kids TLD is restricted to registrants who expressly adhere to the following Guiding Principles in the provision of content and services with their .kids domain:

1) Strictly adhere to the UNCRC principles in the provision of content and services under the .kids domain;

2) Content, including the domain name itself, and services provided through the .kids domain must be appropriate for children under the age of 18 and must not include any materials related to:
- Gambling

- Illegal drugs
- Pornography & Obscenity
- Violence
- Alcohol
- Tobacco
- Criminal Activities;

3) Illegal content is strictly prohibited (including but not limited to trafficking, substance of abuse, phishing, copyright infringement, and other illegal content as defined by the laws of the country for which the registrant and/or the sponsoring registrar resides); and,

4) Registrants pledge to use best efforts basis to offer kids friendly content and services (i.e. content that are more easily comprehendible for kids) on the .kids domain.

Pre-verification processes will be simplified gradually with increased post-registration enforcement supported by anti-abuse measures as described above and in our application #28 Abuse Prevention and Mitigation.

We are prepared to explore to include additional safeguards and moderate the pre-verification processes where appropriate in consultation with ICANN and the GAC.

7. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.

We are supportive of, fully prepared to be, and believe that our proposal is already compliant with the advice.

As mentioned in 4. above, we have already identified various relevant authorities, organizations and bodies to refer to for various processes, including to assess authenticity and consider appropriateness of activities for domain registrations.

Many countries across the world have a children's commissioner or its equivalent. Based on our initial survey, there are Child Commissioners established in 70 countries in over 200 regions. The DotKids Foundation will seek to establish a relationship with them and will consult with them as the relevant national supervisory authority.

As an example, with reference to the European Network of Ombudspersons for Children (ENOC), independent human rights institutions for children from 23 countries in Europe includes:

Member list of ENOC

Armenia	Office of the Human Rights Defender of the Republic of Armenia

Austria	Ombudsperson for Children Province of Vorarlberg - Austria
Azerbaijan	Office of Commissioner for Human Rights of the Republic of Azerbaijan
Belgium	Children's Rights Commissioner - Belgium (Flemish) Délégué général de la Communauté française aux droits de l'enfant
Bosnia and Herzegovina	Ombudsman for children of Republika Srpska The Human Rights Ombudsman of Bosnia and Herzegovina
Croatia	The Ombudsperson for Children Republic of Croatia
Cyprus	Commissioner for Children's Rights of the Republic of Cyprus
Denmark	Danish Council for Children's Rights
Estonia	Chancellor of Justice-Children's Rights Department
Finland	Ombudsman for children in Finland
France	Défenseur des Droits-Défenseur adjoint aux droits des enfants
Georgia	The Office of the Public Defender of Georgia
Greece	Independent Authority Ombudsman of the Hellenic Republic Department of Childrens Rights - Greece
Hungary	Commissioner for Fundamental Rights - Hungary
Iceland	Ombudsman for Children - Iceland
Ireland	Ombudsman for Children - Ireland
Italy	National Authority for Children and Adolescents-Italy
Latvia	Ombudsman of the Republic of Latvia - Children`s Rights Department
Lithuania	Ombudsperson for Children's Rights - Lithuania
Luxembourg	Ombudscommittee for the Rights of the Child - Luxembourg
Malta	Commissioner for Children - Malta
Moldova, Republic of	The Center for Human Rights
Montenegro	Protector of Human Rights and Freedoms of Montenegro
Netherlands	De Kinderombudsman
Norway	Ombudsman for Children - Norway
Poland	Ombudsman for Children-Poland
Russian Federation	Ombudsman for Children under the President of the Federation of Russia
Serbia	Protector of Citizens, Serbia The Provincial Ombudsman-Autonomous Province of Vojvodina
Slovakia	Office of The Public Defender of Rights - Slovak Republic
Slovenia	Slovenia Human Rights Ombudsman Office
Spain	Office of the Catalan Ombudsman-Deputy Ombudsman for Children's Rights Children's Ombudsman in Andalusia-Spain Valedor do Pobo de Galicia
Sweden	Ombudsman for Children in Sweden
Ukraine	The Ukrainian Parliament Commissioner for Human Rights
United	Children's Commissioner for Wales - UK

Kingdom	Office of the Children's Commissioner for England-UK Northern Ireland Commissioner for Children and Young People Scotland's Commissioner for Children and Young People

The fundamental guiding principles of DotKids Foundation , i.e. UNCRC has been ratified by the most countries among all of the Convention than any other human rights treaty in history whereby 192 countries had become State Parties to the Convention as of November 2005. Only two countries, Somalia and the United States, have not yet ratified this celebrated agreement. Somalia is currently unable to proceed to ratification as it has no recognized government. By signing the Convention, the United States has signalled its intention to ratify. (Reference Link: http://www.unicef.org/crc/index_30229.html)

In each of the State Parties, there are dedicated departments within the government to be responsible on monitoring and reporting the implementation situation of the UNCRC within the country whom would be one of the national supervisory bodies that we can work with and seek advice from. Many countries have also established Children's Ombudsman, Children's Commissioner, Child Advocate, Children's Commission or equivalent bodies.

We are prepared to explore to include additional safeguards and to identify and work closely with other relevant authorities where appropriate in consultation with ICANN and the GAC.

8. The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

We are supportive of, fully prepared to be, and believe that our proposal is already compliant with the advice.

That being said, we again emphasize that within the current ICANN gTLD Registry-Registrar framework, the Registry should rely on the Sponsoring Registrar to connect with registrants. Many Registrars feel that it is inappropriate for the Registry to directly contacting the registrant. Therefore, while we will proactively check compliance, in terms of enforcement, we intend to work closely with Registrars to administer corrective measures.

Furthermore, we will develop and implement processes for community, industry and/or public reporting of compliancy issues. These have been included in our responses to #18c, #22, #28 and #29 of our application.

Most importantly a Monitoring Committee will be setup which will continuously conduct post-registration checks to ensure registrants' validity and compliance with requirements:

Monitoring Committee

The Monitoring Committee consists of members of the Foundation, individuals from the Professional Advisory Council and other qualified children's rights, children services or children centric organization who volunteers to be on the notification list. Each Committee Member will be able to login to the complaint-response portal and place a "vote": Red, Yellow or Green against a complaint report filed:

Content Violation Indicators

Red: The domain has severely violated the .Kids Guiding Principles developed by the DotKids Foundation and the domain should be taken down.

Yellow: The domain has marginally violated the .Kids Guiding Principles, a warning should be given and if changes are not made and violation rectified in 10 calendar days, the website should be taken down.

Green: The website did not violate the .Kids Guiding Principles and no action should be made.

The .Kids Guiding Principles have been included in the response to 6. Above and also in the response to #20e Registration policies in the original application.

We are prepared to explore to include additional safeguards and processes where appropriate in consultation with ICANN and the GAC.