📖 **DPGAlliance** / **dpg-standard**   `Public`

<> **Code**   ⊙ Issues **13**   ⑂ Pull requests **1**   ▷ Actions   ⊞ Projects   📖 Wiki   ⚠ Securit

dpg-standard / **standard.md** 📋   ···

👤 **Lucyeoh** Remove the example and link to the Principles for Digital Development   ···   ✓

678f7cf · 8 months ago 🕐

22 lines (19 loc) · 4.45 KB

| Preview   Code   Blame | Raw 📋 ⬇ | ✎ ▾ |

Digital Public Goods Standard

- **Version**: 1.1.4
- **Last Update**: 2021-01-04
- [View Changelog](View%20Changelog)

Indicator	Requirement
1. Relevance to Sustainable Development Goals	Digital public goods must demonstrate relevance to advancing the [Sustainable Development Goals (SDGs)](Sustainable%20Development%20Goals%20(SDGs)).
2. Use of Approved Open Licenses	Digital public goods must demonstrate the use of an approved open license. For open-source software, only [OSI approved licenses](OSI%20approved%20licenses) are accepted. For open content collections the use of a [Creative Commons license](Creative%20Commons%20license) is required. DPGs are encouraged to use a license that allows for both derivatives and commercial reuse ([CC-BY](CC-BY) and [CC-BY-SA](CC-BY-SA)), or dedicate content to the public domain ([CC0](CC0)); licenses that do not allow for commercial reuse ([CC-BY-NC](CC-BY-NC) and [CC-BY-NC-SA](CC-BY-NC-SA)) are also accepted. For open data, an [Open Data Commons approved license](Open%20Data%20Commons%20approved%20license) is required. See [The full license list](The%20full%20license%20list) for reference.

Indicator	Requirement
3. Clear Ownership	Ownership of assets that the digital public good produces must be clearly defined and documented. For example, through copyright, trademark or other publicly available information.
4. Platform Independence	When the digital public good has mandatory dependencies that create more restrictions than the original license, proving independence from the closed component(s) and/or indicating the existence of functional, open alternatives that can be used without significant changes to the core product is required.
5. Documentation	Digital public goods require documentation of the source code, use cases, and/or functional requirements. For content collections, this should include all relevant/compatible apps, software, or hardware required to access the content collection, and instructions regarding how to use it. For software solutions, this should be technical documentation that would allow a technical person unfamiliar with the project to launch and run the software. For data projects, this should be documentation that describes all the fields in the set, and provides context on how the dataset was collected, and how it should be interpreted.
6. Mechanism for Extracting Data and Content	Digital public goods with non-personally identifiable information (PII) design for possibility of extracting or importing non-PII data and content from the system in a non-proprietary format.
7. Adherence to Privacy and Applicable Laws	Digital public goods must be designed and developed to comply with privacy and other applicable laws
8. Adherence to Standards & Best Practices	Digital public goods must be designed and developed to align with relevant standards, best practices, and/or principles.
9. Do No Harm By Design	Digital public goods must be designed to anticipate, prevent, and do no harm by design.

Indicator	Requirement
9a) Data Privacy & Security	Digital public goods that collect, store and distribute [personally identifiable (PII) data](#), must demonstrate how they ensure the privacy, security and integrity of this data in addition to the steps taken to prevent adverse impacts resulting from its collection, storage and distribution.
9b) Inappropriate & Illegal Content	Digital public goods that collect, store or distribute content must have policies identifying inappropriate and illegal content such as child sexual abuse materials in addition to processes for detecting, moderating, reporting and removing inappropriate/ illegal content.
9c) Protection from Harassment	If the digital public good facilitates interactions with or between users or contributors there must be a process for users and contributors to protect themselves against grief, abuse, and harassment. The project must have system(s) to address the safety and security of underage users.

NOTE: Evidence for requirements 7-9 can only be given by someone authorized to speak on behalf of the project. We collect title, name and contact information to confirm this authority.