Draft Coordinated Assessment Data Sharing Agreement and Data Use Policy

**Sixth DRAFT**

March 28, 2014

Chris Wheaton, StreamNet

This draft reflects changes made based on input at the CAPG meeting 3/13/14. Substantive changes include; restricting applicability to CA data and metrics only and requesting consensus and universal application on two issues. Reviewers are asked to provide suggested edits and additional thoughts on content. Send comments to Chris Wheaton, CWheaton@psmfc.org.

This Data Sharing Agreement (DSA) template is intended for use with Coordinated Assessment (CA) data sets that have passed QA, and are ready for dissemination online through StreamNet or the proposed EPA node. The system would stipulate one of two possible levels for sharing.

Under **level one**, data users would be allowed free access under a standard data use policy. For data posted on StreamNet or on the proposed EPA node, this would be similar to the process used to access most data through our website currently. At this level StreamNet would simply post the current data access policy on the StreamNet website (as PTAGIS does). Data contributors would be expected to comply with posted basic standards for data quality, review, etc. Data users would be expected to comply with posted basic standards on use. StreamNet can implement this level either with or without a basic “acknowledgement” step. If acknowledgement is desired, the data user would access the site, enter into one or more interactions where they were told about the data use policy, and upon clicking an “accept” or “agree” acknowledgement, would then be allowed access. We propose not having such a step, but if group consensus is that we need one, that is easily implemented. However, we propose that all level 1 CA data be accessible in the same way. A decision is needed on this issue.

**Level two** would allow data contributors to impose restricted access to specific data fields in any of the CA DES. We are proposing that data contributors develop consensus around the specific fields in each DES where restrictions will be imposed, and that the restricted, level 2 access be consistent across all data for those specific fields. This is because data users might be confronted with a situation where the same type of data could have different access levels with repeated and potentially confusing access restrictions applied if each cooperator independently is choosing the data fields to restrict. We recommend that access levels for different fields in the CA DES be set for everyone at the same level, which would be developed by consensus. Because these fields are primarily derived data that have been through multiple levels of review, we suggest that the level for all fields be a consistent level 1, but if consensus determined that some fields should be level 2, this can be accommodated. A consensus decision is needed designating any restricted access data fields in each DES.

If certain CA DES data fields will be labeled level 2, each agency or tribe will need to provide their own Data Sharing Agreement or limitation of use language. Contributors implementing restrictions could base their language on their own existing state, agency, or tribal policy. The data contributor could choose to define parameters including the appropriate and/or inappropriate uses for the data set. If a funding agency had the need, they could work out specific data sharing agreement language and requirements that they could ask all of their contractors to comply with. Any issues involving disagreement over data sharing would be a contractual issue between funder and contractor.

When accessing level 2 data, the data user would be asked to acknowledge acceptance of the terms of all the agreements on file through a check box acknowledgement step. By accepting the DSA, the requester would acknowledge that they understand the applicable agreements and agree to the terms and conditions specified by any and all of the data contributors. Failure to acknowledge acceptance by clicking an “accept” or “agree” acknowledgement would cause the data to remain inaccessible. At that point the potential data user would be directed to a list of contacts for further discussion.

|  |  |  |
| --- | --- | --- |
|  | **Input** to DSA form (to be filled out by data contributor/creator/provider) | **Output** – what data requester sees on the website, or when clicks ‘Download’ |
| **Level 1: Open Access or Basic DSA with user acknowledgement** | Anyone may download. No stipulations for required interaction with consumers are necessary. See StreamNet Data Use Policy | See StreamNet Data Use Policy. Users are free to use the data as specified in the policy without further acknowledgement or Data users acknowledge policy and basic data sharing agreement by “clicking” before access |
| **Level 2: Restricted DSA with user acknowledgement** | Customized DSAs, with language provided in a file by the data contributor, is linked to access to specified data fields in each DES. Any contractual requirements imposed are the responsibility of the contributor to include in the DSA. If this option is chosen, data users would have to acknowledge agreement before accessing data. | Upon a request for access to certain restricted data fields in each DES, the data sharing agreement text for all agencies and tribes would be shown to the data user and would require agreement by the user before proceeding. If this option is chosen, and agreement was not forthcoming, the user would be directed to a list of contacts, and access to the data through the repository would be denied.  |

Note; for data sets that include sensitive information (such as private personal information, detailed locations of endangered species, etc.), the data set could either be treated as level 2 or two data sets could be uploaded, one level 2 and the other level 1 with the sensitive data removed.

Please note that a disclaimer for any liability incurred by imposition of the policy, and for enforcement responsibility of the policy by the data repository manager and funding agency, will need to be applied. StreamNet would endeavor to design and maintain access to the data for only those that agreed to comply with the agreements for each data set, but would not accept any liability for the legality of any DSA, for any compliance failure, or any ownership of an enforcement function. Any requirements imposed for data sharing by an agency or funding entity would be a contractual matter and not the purview of StreamNet.

----------------------------

# Draft General StreamNet Data Sharing Agreement Language Level One:

The StreamNet guidelines for sharing and use of StreamNet datasets are as follows:

**Those who submit data:**

1. All data in the StreamNet database have been reviewed by the appropriate Data Contributor, but may be updated at any time if revised information becomes available.
2. Data contributors recognize and accept that data submitted to StreamNet at level one are available to anyone via the StreamNet website.
3. Data contributors are responsible for ensuring that the general StreamNet data use agreement is consistent with the applicable policies and rules of their own agencies and any contractual obligations of their projects.
4. Data contributors should ensure data accuracy with a “QA/QC Validation” in publication of data in the StreamNet DataStore. Publication with QA/QC is a choice of the data owner.
5. In most cases, data collection and management has occurred through the use of public funds and applicable federal, state, or tribal open records rules apply. Data files made available at level one meet open records standards for that data.
6. Corrections, if necessary, should be made in a timely manner. Notification of corrections and/or data updates will be posted on the StreamNet website.
7. StreamNet, PSMFC, and BPA accept no responsibility or obligation to take any specific action should violation of these guidelines occur; but may take measures to further restrict access to ensure violations are not repeated.
8. Data contributors have uploaded links to the Metadata records and associated publications that may discuss the limitations and proper use of the data.
9. If publication permissions are requested contributors have 90 days to respond to review requests.

**Those who use data:**

Data users should be careful to properly credit individuals and agencies when using data, and should follow reputable standards for the use and interpretation of scientific information.

Users must assume responsibility to determine the usability of the data for their purposes. Data users acknowledge the StreamNet database is dynamic. Records can be added, deleted and changed on a frequent basis.

Before publication;

The Data User is expected to contact the appropriate Data Contributor and to maintain a record of contact via email and if necessary phone prior to significant use of data in any publication in order to:

1. Obtain verification, data use limitations and context for data through metadata records.
2. Secure appropriate permissions prior to submission for publication by sending requests to data owners and cc’ing the data publishers or peer review team.
3. Arrange appropriate acknowledgements, citations and/or authorships.

\* Failure to comply with the requirements may result in denial of access to restricted data files in future requests. (Data owners have 90 days to respond to data publication reviews). Data users will be notified of any accusations of failure to comply and have opportunities to defend your action to ensure access.

# Draft General StreamNet Data Sharing Agreement Language Level Two

The StreamNet guidelines for use of StreamNet datasets are as follows:

**Those who submit data:**

1. If restrictions on data use or accessibility are imposed on certain data fields, it is the responsibility of the data contributor to ensure that an appropriate data use agreement regarding access and use are posted to StreamNet. StreamNet will maintain these restrictions through the management of access to data via the StreamNet website and by other means to the best of our ability. However, any enforcement of imposed restrictions is the sole responsibility of the data contributor. StreamNet, PSMFC, and BPA accept no responsibility or obligation to ensure that restrictions are maintained or for enforcement of any restrictions.
2. Data contributors are responsible for ensuring that this data use agreement is consistent with all applicable federal and state statutes and rules, as well as the applicable policies and rules of their own agencies and any contractual obligations of their projects.
3. Data contributors should respond to data user review requests within 90 days including requests for permission to publish.

**Those who use data:**

Data users acknowledge their acceptance of the applicable DSA when accessing data via the StreamNet website. They agree to follow the DSA stipulations when receiving access. Any disagreement or discussion regarding the DSA will be directed to the data contributor. StreamNet, PSMFC, and BPA are under no obligation to ensure that the terms of the DSA are legal or enforceable. Data users should be careful to properly credit individuals and agencies when using data, and should follow reputable standards for the use and interpretation of scientific information.

Before publication;

The Data User is expected to contact the appropriate Data Contributor and to maintain a record of contact via email and if necessary phone prior to significant use of data in any publication in order to:

1. Obtain verification, data use limitations and context for data through metadata records.
2. Secure appropriate permissions prior to submission for publication by sending requests to data owners and cc’ing the data publishers or peer review team.
3. Arrange appropriate acknowledgements, citations and/or authorships.

\* Failure to comply with the requirements may result in denial of access to restricted data files in future requests. (Data owners have 90 days to respond to data publication reviews). Data users will be notified of any accusations of failure to comply and have opportunities to defend your action to ensure access.