Jiglu checklist

System configuration

This is a checklist of the decisions you will need to make to configure a new Jiglu site. It should be used in conjunction with the *Jiglu System Assets Checklist*, which covers the images, legal policies and other assets that you will need to gather when setting up a new system.

This checklist covers:

- Roles and permissions
- Users
- Groups
- Privacy
- Content filtering
- Email processing

Before carrying out most of these actions you will need to log in as a system administrator by choosing the *Administrator log in* option from the user menu at the top right of the page and entering your system administrator secondary password. To simplify the descriptions of the actions required, the action of selecting the *Save* button after making a settings change has been omitted from descriptions.

More detailed information on carrying out these tasks can be found in the *Configuring Jiglu* space at support.jiglu.com.

Roles and permissions

Administrators

Are there additional users that you want to allow to modify system permissions and system settings?

This will give them access to carry out any action in the system.

☐ **Yes**

Go to the *Users* section, edit each of these users and give them the *System administrator* role.

☐ **No**

Do you want to allow some users to administer users without giving them full system administrator rights?

This will give them access to create new users, approve users that have registered, change user preferences and deactivate existing users.

☐ **Yes**

Go to the *Roles* system settings category and then select the *New* button. Enter a role name of 'Users administrator', choose the *System* level and then the *Add* button.

Go to the *Permissions* settings category and select the *User* option. For the new *Users administrator* role select all the checkboxes to the right of the role.

Go to the *Users* section, edit each of the users you want to have these rights and give them the *Users administrator* role.

☐ **No**

Do you want to allow some users to administer groups without giving them full system administrator rights?

This will give them access to create new groups, approve new groups or group deletions, change group settings and view all groups.

☐ **Yes**

Go to the *Roles* system settings category and then select the *New* button. Enter a role name of 'All groups administrator', choose the *System* level and then the *Add* button.

Go to the *Permissions* settings category and select the *User* option. For the new *All groups administrator* role select all the checkboxes to the right of the role.

Go to the *Users* section, edit each of the users you want to have these rights and give them the *All groups administrator* role.

☐ **No**

Do you want to allow user administrators to edit users' profiles?

This will give them access to view all profiles and edit the contents of users' profiles.

☐ **Yes**

Go to the *Permissions* settings category and select the *User profile* option. For the new *Users administrator* role select all the checkboxes to the right of the role.

☐ **No**

Users

New users

Do you want to allow anyone to be able to register to use the system?

This will mean anyone visiting the system will be shown a link that takes them to a registration form. They may still need approval afterwards.

☐ **Yes**

Go to the *Permissions* settings category and select the *User* option. Next to the *Guest user* role select the *Add* checkbox.

☐ **No**

Go to the *Permissions* settings category and select the *User* option. Next to the *Guest user* role deselect the *Add* checkbox.

Do you want to allow anyone who is a user of the system to be able to invite other people to join?

This will mean users will see an 'Invite someone to join' option on the home page of a group.

☐ **Yes**

Go to the *Permissions* settings category and select the *User* option. Next to the *Registered user* role select the *Add* checkbox.

☐ **No**

Go to the *Permissions* settings category and select the *User* option. Next to the *Registered user* role deselect the *Add* checkbox.

Do you want individuals who receive an invitation to be reminded if they haven't yet registered?

This will send them a follow-up email in case they missed the invitation the first time.

☐ **Yes**

Go to the *User workflow* settings category and change the *Invitation reminder after* setting to the number of days after which they will receive a reminder.

☐ **No**

Go to the *User workflow* settings category and change the *Invitation reminder after* setting to 0.

Do you want users who register to have their account approved first by an administrator?

This will mean that when a user registers, they do not have access to the system until a system administrator actions a task approving their details. However, if the new user was invited to join by a user with permission to approve users then this check will be skipped.

☐ **Yes**

Go to the *User workflow* settings category and change the *Approve new users* setting to *Yes*.

☐ **No**

Go to the *User workflow* settings category and change the *Approve new users* setting to *No*.

Do you want to allow users who register from certain email domains to have their account automatically approved?

This will mean that a system administrator will not need to action an approval task when users register with an email address from approved organisations. The user will need to have already confirmed they have access to that email address by responding to a message sent to it.

☐ **Yes**

Go to the *User workflow* settings category and for the *Pre-approved domains* setting enter a comma-separated list of the domain names.

☐ **No**

Go to the *User workflow* settings category and make sure the *Pre-approved domains* setting is empty.

Do you want to prevent new users from being able to add new content until a certain amount of time has passed?

This can be useful to enforce a cooling-down period for new users and reduce the potential for abusive behaviour.

☐ **Yes**

Go to the *User limits* settings category and change the *New user action delay* setting to the number of hours until they are allowed to contribute.

☐ **No**

Go to the *User limits* settings category and change the *New user action delay* setting to 0.

User security

Do you want users authenticated in an external LDAP directory?

When a user logs on their password will be checked at an LDAP directory instead of using Jiglu's own authentication system.

☐ **Yes**

Go to the *LDAP directory* settings category, change the *LDAP directory* setting to *Optional* or *Mandatory* and enter the directory access details.

☐ **No**

Go to the *LDAP directory* settings category and change the *LDAP directory* setting to *Off*.

Do you want users to always use two-factor security when logging in?

This will mean that when a user first logs on they will have to set up two-factor authentication using Google Authenticator or a similar app.

If they lose access to the app or the two-factor details then an administrator will need to reset the secret key for their account before they can get access again.

☐ **Yes**

Go to the *User security* settings category and change the *Two-factor security* setting to *Mandatory*.

☐ **No**

Go to the *User security* settings category and change the *Two-factor security* setting to *Optional* or *Off*.

Do you want users to be able to automatically log in without needing to use a password each time?

This will mean that a cookie is stored in a user's browser that will automatically log them on each time. It will remain valid until they change their password or the user account is deactivated.

☐ **Yes**

Go to the *User security* settings category and change the *Automatic log in* setting to *Yes*.

☐ **No**

Go to the *User security* settings category and change the *Automatic log in* setting to *No*.

Do you want to lockout users if they make too many unsuccessful attempts to log in?

This will prevent brute force attempts at getting into an account by repeatedly trying to log in. When an IP address has tried more than a certain number of times it will be prevented from making further attempts for a specified time.

☐ **Yes**

Go to the *User security* settings category and change the *Log in failures before lockout* setting to the required number.

☐ **No**

Go to the *User security* settings category and change the *Log in failures before lockout* setting to 0.

Do you want to limit what times the system is available for users?

This will stop users logging in during certain hours every day or at the weekend, except for system administrators and those with a specific role. This can give extra security at times when the system is not being actively monitored.

☐ **Yes**

Go to the *User limits* settings category and change the *Start time* and *End time* settings to the hours the system is available and *Available weekends* to whether weekends are available too.

☐ **No**

Go to the *User limits* settings category and change both the *Start time* and *End time* settings to midnight and *Available weekends* to *Yes*.

Do you want to enforce a minimum password strength?

This will mean that a user cannot set a new password unless the mixture of letters, numbers and punctuation in it is sufficient to meet the required strength.

This will not be used when an LDAP directory provides authentication

☐ **Yes**

Go to the *User security* settings category and change the *Minimum password strength* setting to the required strength.

☐ **No**

Go to the *User security* settings category and change the *Minimum password strength* setting to *Very weak*.

Do you want to limit how many times each day a user can change their password?

This can stop users repeatedly changing their password so they can reuse an earlier password.

This will not be used when an LDAP directory provides authentication.

☐ **Yes**

Go to the *User security* settings category and change the *Maximum password changes per day* setting to the number of times.

☐ **No**

Go to the *User security* settings category and change the *Maximum password changes per day* setting to 0.

Do you want to prevent users from being able to reuse passwords?

This will ensure users don't keep using the same passwords.

This will not be used when an LDAP directory provides authentication.

☐ **Yes**

Go to the *User security* settings category and change the *Allow password reuse after* setting to how many you want to retain.

☐ **No**

Go to the *User security* settings category and change the *Allow password reuse after* setting to 0.

Do you want to allow users that have forgotten their password to be able to request an email with a link that lets them set a new password?

This will mean as long as they have access to the email account they registered with then they will be able to change the password to recover access. If you cannot guarantee the security of their email service then you may not want to enable this.

This will not be used when an LDAP directory provides authentication.

☐ **Yes**

Go to the *User security* settings category and change the *Forgotten password request link email* setting to *Yes*.

☐ **No**

Go to the *User security* settings category and change the *Forgotten password request link email* setting to *No*.

When users have forgotten their password, do you want to hide the existence of accounts during the recovery process?

This will mean that if someone requests a link to get a new password they will just get a generic message telling them an email has been sent instead of being given more details about what to do or other reasons they are denied access.

This will not be used when an LDAP directory provides authentication.

☐ **Yes**

Go to the *User security* settings category and change the *Keep account existence secret* setting to *Yes*.

☐ **No**

Go to the *User security* settings category and change the *Keep account existence secret* setting to *No*.

Do you want to lockout users if they make too many requests for an email with a link that lets them set a new password?

This will prevent abuse of the password recovery process to flood a user with email. When an IP address has tried more than a certain number of times it will be prevented from making further attempts for a specified time.

☐ **Yes**

Go to the *User security* settings category and change the *Password requests before lockout* setting to the required number.

☐ **No**

Go to the *User security* settings category and change the *Password requests before lockout* setting to 0.

Do you want an administrator to approve any changes of email address?

This will allow a user to change their main email address themselves, but after they have confirmed that they have access to the new account an administrator will still need to action a task to approve the change.

☐ **Yes**

Go to the *User workflow* settings category and change the *Approve new email address* setting to *Yes*.

☐ **No**

Go to the *User workflow* settings category and change the *Approve new email address* setting to *No*.

Do you want users to have their accounts automatically deactivated if they have not logged in for a certain number of days?

Users will receive a warning email if they have not logged in for the number of days you have chosen. If they still do not log in then after a further number of days you have chosen their account will be automatically deactivated. They will then need to contact an administrator to have their account reactivated if they wish to regain access.

☐ **Yes**

Go to the *User workflow* settings category and change the *Send warning if not logged in for* setting to the number of days after which they will get a warning and the *Deactivate user if not logged in for* setting to the number of days after that when their account will be deactivated.

☐ **No**

Go to the *User workflow* settings category and change the *Send warning if not logged in for* and *Deactivate user if not logged in for* settings to 0.

Do you want users to have their accounts automatically deactivated if email to them cannot be delivered?

After email to a user has been bouncing for a certain number of days their account will be automatically deactivated. They will then need to contact an administrator to have their account reactivated if they wish to regain access.

☐ **Yes**

Go to the *User workflow* settings category and change the *Deactivate user if email deactivated for* setting to the number of days after their email was deactivated that their account will also be deactivated.

☐ **No**

Go to the *User workflow settings* category and change the *Deactivate user if email deactivated for* setting to 0.

User defaults and limits

Do you want new users to get a daily summary newsletter?

This will subscribe new users to a newsletter with information about what happened the previous day unless they choose to opt out. If you choose not to enable this the user can always opt in themselves.

☐ **Yes**

Go to the *User defaults* settings category and change the *Default to receive daily summary newsletter* setting to *Yes*.

☐ **No**

Go to the *User defaults* settings category and change the *Default to receive daily summary newsletter* setting to *No*.

Do you want users to have an option over whether to just write plain text or use HTML when entering new discussion messages, and blog comments?

Users may find it simpler to write discussion messages and blog comments in plain text.

☐ **Yes**

Go to the *User defaults* settings category and change the web preferences defaults for each of these contribution types to allow your preferred choices.

☐ **No**

Go to the *User defaults* settings category and change the web preferences defaults for each of these contribution types to remove any choices.

Do you want to put limits on how many new content drafts or submissions a user can create?

This gives protection against malicious users who create huge numbers of content items to try to flood the system.

☐ **Yes**

Go to the *User limits* settings category and change the *Maximum drafts*, *Maximum draft revisions* and *Maximum submissions per day* settings to a sensible maximum, such as 50.

☐ **No**

Go to the *User limits* settings category and change the *Maximum drafts*, *Maximum draft revisions* and *Maximum submissions per day* settings to no limit.

Do you want to log all attachment downloads?

This will allow blog, space and system administrators to see what attachments are being downloaded in the activity log.

☐ **Yes**

Go to the *User limits* settings category and change the *Log downloads* setting to *Yes*.

☐ **No**

Go to the *User limits* settings category and change the *Log downloads* setting to *No*.

Do you want to set a daily download quota?

This will protect against unauthorised bulk downloading of attachments and shared files. Once they hit the limit they will no longer be able to download more until the following day and this will be recorded in the activity log and administrator newsletter.

☐ **Yes**

Go to the *User limits* settings category and change the *Daily download quota* setting to a suitable level for your site, for example 100MB per day.

☐ **No**

Go to the *User limits* settings category and change the *Daily download quota* setting to 0.

Groups

Group creation and deletion

Do you want anyone who is a user of the system to be able to create a group?

This will mean that group creation isn't just limited to system administrators. The group may still need approval afterwards.

☐ **Yes**

Go to the *Permissions* settings category and select the *All groups* option. Next to the *Registered user* role select the *Add* checkbox.

☐ **No**

Go to the *Permissions* settings category and select the *All groups* option. Next to the *Registered user* role deselect the *Add* checkbox.

Do you want new groups to be approved by an administrator before they are activated?

This will mean that when a new group is created its creator will not have access to it until a system administrator actions the task to approve the new group. System administrators creating groups won't be subject to approval.

☐ **Yes**

Go to the *Group workflow* settings category and change the *Approve new groups* setting to *Yes*.

☐ **No**

Go to the *Group workflow* settings category and change the *Approve new groups* setting to *No*.

Do you want the deletion of groups to be approved by an administrator before they are physically removed?

This will mean that if a group administrator decides to delete their group a system administrator will still need to give final approval. This can help protect against accidental or malicious group deletion.

☐ **Yes**

Go to the *Group workflow* settings category and change the *Approve group deletion* setting to *Yes*.

☐ **No**

Go to the *Group workflow* settings category and change the *Approve group deletion* setting to *No*.

Do you want deleted groups to be first suspended for a period of time before they are physically removed?

This will mean that if a group administrator decides to delete their group there is a short period when it can still be returned to use. This can help protect against accidental or malicious group deletion.

☐ **Yes**

Go to the *Group workflow* settings category and change the *Suspend before final deletion* setting to a suitable number of days.

☐ **No**

Go to the *Group workflow* settings category and change the *Suspend before final deletion* setting to 0.

Do you want groups to be marked with one of your organisation's official security access levels so people know who it is appropriate for?

Group categories can be used to provide any information about the type of group, including security levels. When a new group is added the creator will be asked to select from the list of categories for the group.

The categories assigned to a group will be shown in the blog, space and monitor indexes and on the home page of the group.

☐ **Yes**

Go to the *Group categories* settings category, select the *New* button and enter the name and optional description of the category that you wish to add.

Group limits and feature availability

Do you want to prevent group administrators from changing the text of group notification messages?

This will stop group administrators changing notifications to things that don't make sense or that may confuse their members.

☐ **Yes**

Go to the *Group defaults* settings category, choose the *Category visibility group defaults* option and then change every notification category to *Invisible*.

☐ **No**

Go to the *Group defaults* settings category, choose the *Category visibility group defaults* option and then change every notification category to *Not set*.

Do you want to prevent group administrators from having access to certain advanced group settings like resource permissions, filtering, workflow or tagging?

This will mean that group administrators won't see these categories in the group settings. This can be useful to simplify what most administrators can do with their groups.

If you want to allow a specific group to have access to a category then you can edit the visibility settings for that group.

☐ **Yes**

Go to the *Group defaults* settings category, choose the *Category visibility group defaults* option and then change these categories to *Invisible*.

☐ **No**

Go to the *Group defaults* settings category, choose the *Category visibility group defaults* option and then change these categories to *Not set*.

Do you want to prevent group administrators from having access to certain settings but still allow them access to everything else in a settings category?

This will mean that when a group administrator goes to the settings category containing the setting they will still be able to see what it is set to but won't be able to change it.

☐ **Yes**

Go to the *Group defaults* settings category, choose the category where the setting is found and select the checkbox next to the lock icon.

☐ **No**

Go to the *Group defaults* settings category, choose the category where the setting is found and deselect the checkbox next to the lock icon.

Do you want to limit how much storage a blog or space is allowed to use?

This will mean that when a group hits its maximum storage size no more content can be added to it until some of the existing content is removed.

If you want to allow a specific group to have more space then you can edit the quota settings for that group.

☐ **Yes**

Go to the *Group defaults* settings category, choose the *Limits and quotas* option and set the *Hard limit* setting to the maximum content storage you want the group to use.

For a space, if you want old messages to be expired when a limit is reached then set a *Soft limit* size, for *Purge when hit quota* select *Yes* and then how much you want to expire each time – 10% is a good starting point.

☐ **No**

Go to the *Group defaults* settings category, choose the *Limits and quotas* option and set the *Hard limit* setting to 0.

Do you want to limit how many of a particular type of resource (such as a source or a newsletter) a group is allowed to create?

This gives protection against malicious users who create huge numbers of resources to try to flood the system.

☐ **Yes**

Go to the *Group defaults* settings category, choose the *Limits and quotas* option and set the limit for each type of resource to an appropriate default, such as 20.

☐ **No**

Go to the *Group defaults* settings category, choose the *Limits and quotas* option and set the limit for each type of resource to *No limit*.

Do you want group administrators to be allowed to force members to subscribe to a newsletter?

This will mean that if a group administrator creates a mandatory newsletter then users will have no choice over whether or not to receive it.

☐ **Yes**

Go to the *Group limits* settings category and change the *Allow mandatory newsletters* setting to *Yes*.

☐ **No**

Go to the *Group limits* settings category and change the *Allow mandatory newsletters* setting to *No*.

Privacy

Do you want ordinary users to be able to view the index of users?

If the system is being used by users from multiple organisations then you may want to limit who can view the user index. Users will still be able to view the profiles of users that create content but not those who choose not to.

☐ **Yes**

Go to the *Permissions* settings category and select the *Users* option. Next to the *Registered user* role select the *View* checkbox.

☐ **No**

Go to the *Permissions* settings category and select the *Users* option. Next to the *Registered user* role deselect the *View* checkbox.

Do you want ordinary users to be able to see other users' email addresses?

If the system is being used by users from multiple organisations then you may want to limit who can view email addresses. If someone creates a discussion message that is sent by email to members of a space then it will still contain their email address.

☐ **Yes**

To change whether email addresses are shown on system pages go to the *Appearance* settings category and change the *Show email addresses* setting to *Yes*.

To change whether email addresses are shown by default in a group go to the *Group defaults* settings category, choose the *Privacy* option and change the *Show email addresses* setting to *Yes*. If you don't want group administrators to change this setting then select the checkbox next to the lock icon.

☐ **No**

To change whether email addresses are shown on system pages go to the *Appearance* settings category and change the *Show email addresses* setting to *No*.

To change whether email addresses are shown by default in a group go to the *Group defaults* settings category, choose the *Privacy* option and change the *Show email addresses* setting to *No*. If you don't want group administrators to change this setting then select the checkbox next to the lock icon.

Do you want search engines to index public pages on the site?

Private pages will never be visible to search engines, but if you're using Jiglu for an internal purposes then you may not want search engines to index the landing page or any pages that might be public.

☐ **Yes**

Go to the *Page elements* settings category and change the *Robots meta tag* setting to be empty.

☐ **No**

Go to the *Page elements* settings category and change the *Robots meta tag* setting to 'noindex, nofollow'.

Content filtering

Do you want to restrict attachments and file sharing to only certain media types?

If the system is being used by users from multiple organisations then you may want to limit who can view the user index. Users will still be able to view the profiles of users that create content but not those who choose not to.

☐ **Yes**

Go to the *Filtering* settings category, scroll down to the bottom of the *Filter out attachments of these media types* setting and select all the entries under the *Wildcards* section. Now in the *Unless they are of one of these media types* setting choose the attachment types that you want to allow. Finally, change the *Allow attachments with unknown media types* setting to *No*.

☐ **No**

Go to the *Filtering* settings category and ensure nothing is selected in the *Filter out attachments of these media types* setting or the *Unless they are of one of these media types* setting. Finally, change the *Allow attachments with unknown media types* setting to *Yes*.

Do you want to restrict users from using external images, videos and audio in their contributions?

If you allow external content then the server that it is hosted on may be able to get information about who is viewing it and there could be a security risk for certain kinds of content. With blocking of media from unknown external sites enabled, only sites that are listed in the Embedded sites *settings category can have their content used.*

☐ **Yes**

Go to the *Filtering* settings category and change the *Block media from unknown external sites* setting to *Yes*.

To add a site that you want to allow content from, go to the *Embedded sites* setting category, select the *New* button and add the details of the site.

To deactivate a default embedded site which you don't want to allow content to be used from, go to the *Embedded sites* setting category, select the site and change the *Status* to *Deactivated*.

☐ **No**

Go to the *Filtering* settings category and change the *Block media from unknown external sites* setting to *No*.

Do you want to allow users to embed videos from YouTube, documents from Google Docs or embeddable content from other sites in their contributions?

If you allow embeddable content then the server that it is hosted on may be able to get information about who is viewing it and there could be a security risk for certain kinds of content. Only sites that are listed in the Embedded sites settings category can have their content embedded.

☐ **Yes**

Go to the *Embedded sites* setting category and check to see if the site already exists and that it has its status set to *Activated*. To add a new site, select the *New* button and add the details of the site.

☐ **No**

To deactivate default embedded sites which you don't want to allow content to be embedded from, go to the *Embedded sites* setting category, select each site in turn and change the *Status* to *Deactivated*.

If you prefer to delete them select the checkbox next to each name and then the *Delete* button.

Do you want to have links to YouTube or other media converted into the actual video on the page?

This will mean that rather than having to follow the link to view the video or see the media it can be viewed inline in the contribution.

☐ **Yes**

Go to the *Filtering* settings category and change the *Automatic content embedding* setting to *Yes*.

☐ **No**

Go to the *Filtering* settings category and change the *Automatic content embedding* setting to *No*.

Do you want attachments and shared files to be scanned for viruses?

You will need to have a virus scanner that supports the ICAP protocol. When virus scanning is enabled users will be unable to download files until after they have been scanned for viruses.

☐ **Yes**

Go to the *Virus scanning* settings category, change the *Enabled* setting to *Yes* and enter the details of the ICAP server used for virus scanning.

☐ **No**

Go to the *Virus scanning* settings category and change the *Enabled* setting to *No*.

Do you want to restrict certain words, such as profanity, from being used in discussion messages or blog comments?

If you have groups with public content that anyone can contribute to then you may wish to put in controls against abusive language.

Blog and space workflow settings for these contribution types will also need to be configured to choose an appropriate action when such words are found. A talk filtering setting will control whether such words are allowed in instant messages.

☐ **Yes**

Go to the *Banned words* settings category and paste a list of the words that you do not want to appear.

☐ **No**

Go to the *Banned words* settings category and remove the list of words.

Email processing

Do you want non-delivery notifications to be automatically handled by the system?

With bounce processing enabled, the system will deactivate email for users when messages cannot be successfully delivered to them. They will not be able to contribute until they have confirmed they can successfully receive messages once more.

☐ **Yes**

Go to the *Bounce processing* settings category and change the *Automatic bounce processing* setting to *Yes*.

☐ **No**

Go to the *Bounce processing* settings category and change the *Automatic bounce processing* setting to *No*.

When a non-delivery notification for a discussion message or group newsletter cannot be processed, do you want it to be sent to a system administrator rather than the group administrator?

The administrator of a group might want to know if messages can't be sent to a member but if they're not also a system administrator then they won't be able to take any action other than removing the member from the group.

☐ **Yes**

Go to the *Bounce processing* settings category and change the *System administrators get group bounces* setting to *Yes*.

☐ **No**

Go to the *Bounce processing* settings category and change the *System administrators get group bounces* setting to *No*.

Do you want non-delivery notifications to go to a specific email address instead of to the system administrators?

For a system with a lot of users the number of non-delivery notifications might get annoying so they can instead be directed to a dedicated mailbox which administrators can then process.

☐ **Yes**

Go to the *Bounce processing* settings category and change the *Bounce notification address* setting to the required email address.

☐ **No**

Go to the *Bounce processing* settings category and change the *Bounce notification address* setting to be empty.

Do you want email messages for administrators that are potentially spam to still be forwarded on to them?

If a message is misclassified it still might be important to get to an administrator. However, if too many spam messages are forwarded by the server it could affect its reputation.

☐ **Yes**

Go to the *Other processing* settings category and change the *Administrator forwarding includes spam* setting to *Yes*.

☐ **No**

Go to the *Other processing* settings category and change the *Administrator forwarding includes spam* setting to *No*