Site Policies

The Site policies area can be accessed by Site administrators via the **Administration** block within *Site administration > Security > Site policies.*
Site policy options include a range of security settings for both users and the site as a whole.

Settings

Setting	Description	Notes
Protect usernames	If enabled, when a user attempts to reset their password and enters a username or email address, they will see an onscreen message of, 'If you supplied a correct username or email address then an email should have been sent to you.' This is to prevent a malicious party from using the reset functionality to determine which usernames and email addresses are in use in valid accounts. If the protect usernames setting is disabled, when a user attempts to reset their password they are advised whether an account exists with the username or email address supplied. The message 'The email address was not found in the database' will be displayed is no account can be found.	-
Force users to log in	Normally, the entire site is only available to logged-in users. If you would like to make the front page and the course listings (but not the course contents) available without logging in, then you should uncheck this setting. If this setting is enabled, users visiting the site will first be presented with the login page.	**Tip** You can customise the text users see on the right side of the login screen via the **Administration** block within *Site administration > Plugins > Authentication > Manage authentication > Instructions.*
Force users to log in for profiles	This setting forces people to log in as a real (non-guest) account before viewing any user's profile. If you disabled this setting, you may find that some users post advertising (spam) or other inappropriate content in their profiles, which is then visible to the whole world.	-
Force users to log in to view user pictures	If enabled, users must log in in order to view user profile pictures and the default user picture will be used in all notification emails.	-

On this page

Related pages

Prevent multiple logins by the same user	If checked, a user can only login to their account from a single location. If a second account logs in, the first one will be automatically logged out.	**Tip** Enabling multiple logins allows Site administrators to 'log in as' a logged in user while providing live technical support.
Open to Google	If you enable this setting, then Google will be allowed to enter your site as a Guest. In addition, people coming into your site via a Google search will automatically be logged in as a Guest. Note that this only provides transparent access to areas of your site and courses that already allow guest access.	-
Profile visible roles	List of roles that are visible on user profiles and participants pages.	-
Maximum uploaded file size	This specifies a maximum size that uploaded files can be, throughout the whole site. This setting is limited by the PHP settings post_max_size and upload_max_filesize (in php.ini), as well as the Apache setting LimitRequestBody. In turn, maxbytes limits the range of sizes that can be chosen at course level or module level. If **Server Limit**' is chosen, the server maximum allowed by the server will be used. Upload file sizes are restricted in a number of ways and each one in this list restricts the following ones: • Server level • Site level • Course level • Activity level	-
User quota	The maximum number of bytes that a user can store in their own private file area. The default of 04857600 bytes = 100MB.	-
Allow EMBED and OBJECT tags	As a default security measure, normal users are not allowed to embed multimedia (like Flash) within texts using explicit EMBED and OBJECT tags in their HTML (although it can still be done safely using the mediaplugins filter). If you wish to allow these tags then enable this option.	-
Enable Trusted content	By default, Totara will always thoroughly clean text that comes from users to remove any possible bad scripts, media etc that could be a security risk. The Trusted Content system is a way of giving particular users that you trust the ability to include these advanced features in their content without interference. To enable this system, you need to first enable this setting, and then grant the Trusted Content permission to a specific Totara role. Texts created or uploaded by such users will be marked as trusted and will not be cleaned before display.	-

Maximum time to edit post	This specifies the amount of time user have to re-edit forum postings, glossary comments etc. Allowing users this 'cool off' period after submitting a forum/glossary entry post allows them time to review content, check spelling and grammar.	**Note** Forum posts within the editing period are still visible in the correspondi ng forum, but the message will not be sent out to any subscribed users until the edit post period has passed.
Allowed characters in usernames	Enable this setting to allow learners to use any characters in their usernames (note this does not affect their actual names). The default is **No**' which restricts usernames to be alphanumeric lowercase characters, underscore (_), hyphen (-), period (.) or at symbol (@).	**Tip** This option must be enabled for the site to use email addresses for usernames.
Site policy URL	If you have a site policy that all registered users must see and agree to before accessing the rest of the site, then specify the URL to it here, otherwise leave this field blank. The URL can point to any type of file anywhere online that can be accessed without a login to your Totara Learn site. • It is recommended that the site policy is on the same domain as Totara to avoid the problem of Internet Explorer users seeing a blank screen when the site policy is on a different domain. • The site policy will be displayed in a frame. You can view it via the URL *yourtotarasite.com/user/policy.php*. • If Email-based self-registration*i*s enabled on the site, a link to the site policy is displayed on the signup page. It is not recommended that a Page resource is used as a Site policy since the site header will be repeated in the iframe.	-
Site policy URL for guests	If you have a site policy that all guests must see and agree to before using this site, then specify the URL to it here, otherwise leave this field blank. This setting can contain any public URL.	**Note** Access of not-logged-in users may be prevented with forcelogin setting.

Keep tag name casing	Check this if you want tag names to keep the original casing as entered by users who created them. If checked, then tags like the following will be displayed: RUGBY, gUiTaR, totara If unchecked, then all tags will be displayed as follows: Rugby, Guitar, Totara.	**Tip** For English, off is useful. For Japanese, no changes are made either way. For languages where this kind of capitalisation changes the meaning, it is best to keep this option on
Profiles for enrolled users only	To prevent misuse by spammers, profile descriptions of users who are not yet enrolled in any course are hidden. New users must enrol in at least one course before they can add a profile description.	-
Cron execution via command line only	Running the cron from a web browser can expose privileged information to anonymous users. Thus it is recommended to only run the cron from the command line or set a cron password for remote access.	-
Cron password for remote access	This means that the cron.php script cannot be run from a web browser without supplying the password using the following form of URL: http://site.example.com/admin/cron.php?password=opensesame If this is left empty, no password is required.	-
Account lockout threshold	After a specified number of failed login attempts, a user's account is locked and they are sent an email containing a URL to unlock the account. Setting this to **No**' means there is no threshold and an account attempting to log in can do so an unlimited number of times.	-
Account lockout observation window	Observation time for lockout threshold, if there are no failed attempts the threshold counter is reset after this time. This is the counter for how long to watch for more failed attempts by an account trying to log in even after being locked out, the counter will reset at each attempt and last this long.	-
Account lockout duration	Locked out account is automatically unlocked after this duration. An account may also be unlocked by a Site administrator within the **Administration** block *via Site administration > Users > Accounts > Browse list of users.*	-

Password policy	Turning this on will make Totara Learn check user passwords against a valid password policy. It is highly recommended that a password policy is set to force users to use stronger passwords that are less susceptible to being cracked by an intruder. Use the settings below to specify your policy (they will be ignored if you set this to **No**). If a user enters a password that does not meet the requirements, they are given an error message indicating the nature of the problem with the entered password. Enabling the password policy does not affect existing users until they decide to or are required to change their password. An admin can force all users to change their password using the force password change option in Bulk user actions.	**Tip** The password policy may also be applied to enrolment keys by ticking the **Use password policy** checkbox in the Self-enrolment settings
Password length	Passwords must be at least these many characters long.	-
Digits	Passwords must contain these many digits.	-
Lowercase letters	Passwords must contain at least these many lower case letters.	-
Uppercase letters	Passwords must have at least these many upper case letters.	-
Non-alphanumeric characters	Passwords must have at least these many non-alphanumeric characters.	-
Consecutive identical characters	Passwords must not have more than this number of consecutive identical characters. Use 0 to disable this check.	-
Password rotation limit	Number of times a user must change their password before they are allowed to reuse a password. Hashes of previously used passwords are stored in local database table.	**Note** This feature might not be compatible with some external authentication plugins.
Maximum time to validate password reset request	This specifies the amount of time people have to validate a password reset request before it expires. Usually 30 minutes is a good value.	-
Log out after password change	By default, users can change their password and remain logged in. Enabling this setting will log them out of existing sessions except the one in which they specify their new password. This setting only applies to users manually changing their password, not to bulk password changes.	-
Group enrollment key policy	Turning this on will make Totara Learn check group enrolment keys against a valid password policy.	-

Disable user profile images	Disable the ability for users to change user profile images.	-
Email change confirmation	Require an email confirmation step when users change their email address in their profile.	-
Remember username	Enable if you want to store permanent cookies with usernames during user login.	**Warning** This will store permanent cookies and in some countries may be considered a privacy issue if used without consent.
Strict validation of required fields	If enabled, users are prevented from entering a space or line break only in required fields in forms.	-

Password reset behaviour

If you forget your password then you can request a new one. However how this is handled by Totara Learn will depend on if this is your first request or not.

- **First request:** If this is the first reset request then Totara Learn will send the reset email.
- **Subsequent request (first expired):** If this isn't the first reset request, but the previous request has expired (set by the **Maximum time to validate password reset request** setting), then Totara Learn will send a new reset email.
- **Second request:** If this is the second reset request then the system will send the reset email.
- **Third or more request:** If this is the third, or greater reset request then the email will not be resent.

This means that if you forget your password, you can request a reset and re-request a reset, however after that you will have to wait for the previous request to expire.