WordPress Hosting - Research Lab Sites

- Introduction
- Tiers and Fees
- Eligibility
- Requesting Service
- OIT Roles and Responsibilities
- Site Owner Roles and Responsibilities
- User Levels
- Content Restrictions and Advisories
- System Reliability and Maintenance
- System Security
- Secure Site Requirements and Limitations
- Related Articles

Introduction

Franklin College Office of Information Technology (Franklin OIT) may offer free limited support hosting for existing WordPress sites to replace sites currently hosted on unsupported servers housed within Franklin College departments or on EITS Web standard hosting, which is being decommissioned.

These sites will be hosted as is, with no guarantees of support beyond the maintenance of WordPress core, plugins, and the hosting environment. There is no documentation available for managing these sites. No additional technical support is available for this service.

WordPress Core and Plugins

The Franklin OIT WordPress hosting service will support sites "as is" if the site functions within our hosting environment. There are some WordPress sites that require plugins that are not usable in the hosting environment. If the WordPress site operates on Pantheon, and we agree to host the site, the following parameters will apply:

- Sites installed as is.
- All content managers must have a UGA myID or have an approved contractor myID to access the WordPress backend.
- Site owner user account will be an "Editor" level account.
- Site owner will not be able to install any other themes or plugins, and there is no direct FTP access for the sites.
- Plugins and WordPress Core must be patched on a regular basis by Franklin OIT. If patching breaks any part of the site, Franklin OIT is not responsible for, or able to, correct errors. Please contact us for additional elevated access to the testing environment for troubleshooting.
- All sites are limited to 25k monthly visits. Exceeding this visit cap will incur charges.

Tiers and Fees

There are no fees for this service unless your site exceeds the 25k monthly visit caps for more than two months in a row. All fees are paid to the hosting provider.

Franklin OIT does not offer technical support or personal assistance with these sites. The site owner is responsible for maintaining internal documentation and is responsible for training anyone that needs to update the sites.

Eligibility

Wordpress hosting for Research Lab Sites is only available to Active Franklin College Faculty. When a faculty member is no longer an active employee of the University, their site will be disabled. This service is not available for Franklin instructional units.

Requesting Service

This service has limited availability and use cases. Please submit a ticket via http://helpdesk.franklin.uga.edu to request information about this service.

OIT Roles and Responsibilities

OIT will provide the following as part of the CMS service:

1. OIT will import WordPress code and database to the hosting environment.
2. OIT will setup initial site owner accounts and access levels using MyID authentication
3. OIT will appropriate redundant hardware and infrastructure to support these services
4. OIT will ensure security (SSL) certificates are utilized for all secure transmissions
5. OIT will provide one (1) domain name through standard provisioning.
6. OIT will provide temporary elevated testing environment access for troubleshooting in the case that plugin or core updates breaks any part of the site.

Site Owner Roles and Responsibilities

1. Client will manage all content. Franklin OIT does not provide content editing services.
2. Clients will only post content appropriate for these sites.
3. Clients will make every effort to keep content relevant and up to date.
4. Clients will submit request for service through the helpdesk ticketing system available at http://helpdesk.franklin.uga.edu. Alternatively, requests may also be submitted to helpdesk@franklin.uga.edu. Franklin OIT does not provide technical support for this service but help with providing temporary elevated access levels on the testing environment for troubleshooting.
5. Clients should familiarize themselves with InfoSec data policies (https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/) as well as any other relevant data policies.

User Levels

Below is a description of the types of activities performed by the user level provided with these sites.

**Content Administrator access** - All users can access the WordPress web site using their normal MyID as a content manager or editor. Content managers/editors with this level of access are able to perform the basic tasks of making content updates and uploading images (up to 2 MB each).

There is no access to web code under any circumstance.

Content Restrictions and Advisories

Clients are responsible for ensuring that they are authorized to use any copyrighted material that may be posted on their websites. If Franklin OIT receives a copyright infringement notification, we may need to take all or part of the site offline until the issue can be rectified. Faculty or Research Labs must receive permission from students prior to posting images of students on their websites. Content must also adhere to local, state, and federal laws as they apply. Sensitive data may not be stored on the CMS service at any time. The presence of sensitive data will necessitate taking the site offline until all risks have been documented and mitigated.

These sites are not available for Special Events or Student Organizations.

System Reliability and Maintenance

Franklin OIT strives to keep CMS websites in production 24hrs/7days a week. Core upgrades will be performed at regularly scheduled intervals and during hours outside of typical business hours. When necessary, some maintenance may occur during regular business hours. Site owners will be notified of any scheduled or emergency system interruptions.

Occasionally, campus network problems do occur. During these times, please ask your IT professional to work with EITS to resolve or provide updates on these issues. Off-campus website visitors should work with their Internet Service Providers as necessary to resolve off-campus network issues.

System Security

Systems security and protection are of the utmost importance to Franklin OIT. Security measures have been taken to ensure that our systems are protected against unwanted or malicious external access as well as maintaining the integrity of the data being hosted. Clients with access to systems are responsible for keeping their account credentials secure and limited to only their own use. Account credentials will adhere to the University Password Policy and Standard.

Portions of hosted sites which handle sensitive information will be secured using secure socket layers (SSL) with a fully signed certificate issued from the InCommon Certificate Authority (CA). Site code is isolated on the hosting systems through the use of individual security containers per site, to eliminate any possibility of exposure to underlying databases or other sites hosted on the same systems.

Secure Site Requirements and Limitations

All clients will have the login page of their site served over secure socket layer (SSL) using a signed security certificate.

Related Articles

- Franklin OIT Service Offerings