



Information Services

Birkbeck Information Security Policy

Code of Practice 2 – Granting Access to WP Engine to Third Parties

Approved by IT Security and Governance Group

20 July 2022

1. Context

This code of practice forms part of the [Birkbeck IT Regulations](#) and must be read and understood in that context. For more information, contact [Birkbeck IT Services](#), a link to their contact details is available on the [Birkbeck IT Regulations](#) page.

2. Introduction

The purpose of this code of practice is to define standards for all Third Parties seeking to access the College's WP Engine environment where the Third party is an individual or organisation external to the College but contracted by a member of the College to create, develop, support and maintain an approved WordPress web presence within WP Engine.

This code of practice is designed to minimise the potential exposure to the College from risks associated with Third Party access.

This code of practice applies to organisations, third party support suppliers and of organisations partnering with the College requiring access to the College's WP Engine environment.

3. Access Requests

Requests to allow access to the College's WP Engine environment must meet the following criteria:

3.1 An employee of the College who is the sponsor for the activity must make a request for access for the third party via the College's support desk system, [Ask](#). The request must list

named individuals and email addresses such that individualised access can be provided, as well as the name of the specific WordPress site that they will be working on.

3.2 This request must be made at least 9 working days before the access is required to allow time to complete the process.

3.3 The request must be formally authorised by an “Authoriser”, a senior member of staff within the Information Services department, such as the CIO, Head of Infrastructure, Head of Corporate Information & Web Systems or Head of Information Security.

3.4 Access to WP Engine environment for Third Parties will not be provided until a contract or schedule of work has been signed defining the terms and scope for the work and a copy of this contract and/or the agreed schedule of work must be appended to the Ask request.

3.5 Third Party access will be permitted only to the WordPress sites specified in the original request.

3.6 The sponsor is expected to notify the authoriser once the work has been completed and access is no longer required so that it can be disabled.

3.7 The Third Party WP Engine Access Agreement (below) must be signed by all parties before access is granted.

4. Third Party WP Engine Access Agreement

Ask ID	
---------------	--

The following sponsor has requested access to WP Engine for the Third Party individuals listed below and takes responsibility for monitoring their actions

Sponsor Name	Sponsor Email Address	Sponsor Department

The following Authoriser is a member of Information Services staff who will provide access to the WP Engine environment

Authoriser Name	Authoriser Email Address	Authoriser Department

Access start date	
--------------------------	--

Access is granted to the following Third Party individuals:

Name	Email address

To manage the following WordPress sites in WP Engine:

Site name	Site URL

5. Access conditions

5.1 Access to the College’s systems and data is granted for purposes described in the contract or schedule of work only. The use of this access for personal use or gain is strictly prohibited.

5.2 Access to the College’s WP Engine environment will not be provided until a signed copy of this agreement has been returned to the authoriser.

5.3 The Third Party is required to maintain a list of all individuals authorised to use the access and make this available to the College.

5.4 The Third party will inform the College in writing of relevant staff changes. This includes the rotation and resignation of employees so that the College can disable access and remove accounts in order to secure its resources. If new staff need to access the system, this form will need to be resubmitted. Access should be on an individual-by-individual basis - sharing access violates this agreement.

5.5 The Third party must comply with all relevant government legislation including but not limited to the Data Protection Act 2018.

5.6 The College reserves the right to monitor activity and revoke access without giving a reason at any time.

5.7 The College reserves the right to audit contractual responsibilities and to provide any data about this work required in order to discharge audit duties from external partners.

5.8 The Third Party is required not to take any action on systems, sites or data that falls outside of the scope of the work authorised and described in the contract or schedule of work.

5.9 Any suspected security breaches or other incidents must be reported in within 48 hours to the College’s IT Service Desk via Ask.

5.10 The Third Party will, at all times, be held responsible for any activities which occur on College's systems using any unique credentials granted.

5.11 The Third Party is solely responsible for ensuring that any username(s) and password(s) that they are granted remain confidential and are not used by unauthorised individuals.

5.12 When a Third Party is connected to the College's systems they should not leave the machine/device unattended.

5.13 Workstations/laptops that are used to display College's data should be located such that confidential information is not displayed to unauthorised persons or the general public.

5.14 The College reserves the right to increase security thresholds if future security risks are identified.

Signed on behalf of Third Party

Name: _____

Title: _____

Date: _____

I confirm that all the individuals to whom access is granted via this agreement have read, understood and agree to adhere to the terms of this agreement and all related Birkbeck Corporate Policies and IT Regulations.

Signature: _____

Signed on behalf of Birkbeck College, University of London

Sponsor

Name: _____

Title: _____

Date: _____

I confirm that an appropriate contract or schedule of work has been signed for this access:

Signature: _____

Authoriser

Name: _____

Title: _____

Date: _____

Signature: _____

6. Version Control

Version	Date	Author	Comments
1.0	April 2022	Steve Potter	With input from Marion Rosenberg
	July 2022	Approved by	ITSAG