Web Content Governance Policy

Introduction

The university's website is a powerful tool for distributing content to internal and external audiences and is core to enabling the university to communicate and carry out its business. With the responsibility this brings comes a requirement to comply with relevant legislation as well as internal policies, procedures and codes of conduct.

Conforming to such requirements is not optional, but nor should it represent a barrier to the effective delivery of locally-managed and sourced content to all of our key audiences.

This policy covers all content which is deployed through either the website or portal.

The document explains the governance approach taken within the university to ensure:

1) That all content meets the legal obligations of the university with regards to digital communication (e.g. compliance with Data Protection legislation).
2) That all such content meets the aspirations of the university's Strategic Plan, Marketing Strategy, Information and Technology Strategy and other relevant strategies.
3) That all relevant university polices are understood and complied with, including but not limited to the Information Security Policy and Records Management Policy.
4) That all individuals with responsibility or accountability for content compliance have received adequate and regular training and fully understand their role.
5) That content, where relevant, can be managed at a local level within Faculties and Directorates whilst still complying with the above.
6) That quality is maintained so that users of the university's website always have access to accurate, consistent, well-written and current information.

Out of scope: Online academic programme governance

The university is required to meet further legal requirements stipulated by the Consumer Credit Act (CCA) which is overseen by the Competition and Markets Authority (CMA) with regards to its provision of online programme information. To ensure the institution is fully compliant with these additional legislative requirements, responsibility for online governance of all programme pages and related marketing information is covered by a separate policy overseen by the Communications and Recruitment Directorate.

Content workflows

Where appropriate, all online content is subject to workflow to ensure it meets all of our governance objectives. Workflow is generally required when at least one of the following conditions is met:

1) Local content management (i.e. at Faculty or Directorate level) is required.
2) The content is to be locked down as "staff only."
3) Inappropriate management of the content is deemed by the Information Officer or Digital Services Manager to pose a legal or strategic risk to the university.

Exceptions to workflow

Exceptions to workflow can be made in situations where all parties agree that a workflow would be impractical (e.g. due to resource or frequency of update). All exceptions, however, require written sign-off by the relevant Faculty Operating Officer or Director of Professional Services.

Roles and permissions

In order to manage content effectively, the following roles and permissions exist within the university:

Role	Description	Permissions
Content creator	The majority of administrative users on the website. No specialist training required although it is recommended. Content creators are required to agree a relevant period of review for any content they create with their Web Editor. **Appointment must be signed off by Web Editor**	Create content within a designated area.
Content approver	Individuals with **responsibility** for creating and approving content. (e.g. Web Editors) Generally, no more than five approvers will be designated within an individual Faculty or Directorate. **Must have attended and passed annual Online Content Training.** **Appointment must be signed off by Faculty Operating Officer or Director**	Create content within a designated area. Approve (or reject) content within a designated area.
Central Governance officer	Individuals able to override local content decisions where appropriate (e.g. Web Team members and the Information Officer) **Must have attended and passed annual Online Content Training.**	Create content site-wide. Approve content site-wide.
PVCs or Directors	PVCs or Directors are fully	No permission within the

	accountable for the content which is published to the website or portal by content approvers within their Faculty or Directorate.	content management system but management responsibility for relevant content approvers.

For an example of how these roles might be allocated within a faculty, see *Appendix 1: Example Faculty Governance Structure*.

Users and groups

The above roles generally map to a number of specific users or user groups within the university structure.

1) **The Director of ILS** – able to override any governance decision based on the consideration of risk to the institution and/or judgement within the context of the "IT Director" role. This decision can be appealed. *(See appealing a decision below*).
2) **The Information Compliance Manager (VCs Office)** – capable of vetoing any governance action on the part of a creator or approver when s/he feels that action carries a risk of legal or strategic damage to the institution (e.g. carries a risk of contravening the DPA).
3) **The Digital Services Manager** – can refer actions to the Information Compliance Manager or Director of ILS for consideration of legal or strategic issues. Can veto the granting of Creator or Approver users.
4) **Web and Content Team** – **Central Governance Officers** within the university.
5) **Web Editors** – Web editors must **always** be one of their Faculty or Directorate's **Content Approvers**. They must also nominate at least one deputy who must also be a **content approver**. All requests for content creator permissions and training attendance must come via a Web Editor.
6) **Web Authors** – Content creators within individual faculties.
7) **PVCs or Directors** – accountable for the content published by staff within their areas of responsibility.
8) **Communications Consultative Group** – overall responsibility for this and any other policy relating to web content management and its governance.

Faculty vs department approvers

Where a faculty or directorate is considered too large a content grouping to allow the effective management of content in line with the governance objectives, web editors and approvers can be designated at department level.

This requires sign-off by a relevant senior manager and the Director of ILS.

In these situations **all other rules** (such as training requirements and the appointment of deputies) must still be applied, and one Web Editor must be designated as **Lead Web Editor** for administrative and coordination purposes.

Online content training

In order to ensure that individuals placed in an approval role have been given an appropriate level of training and guidance, all prospective approvers **must** attend and pass the

Introduction to Online Content Management training course before taking on the role. Attendance at an annual refresher training event is also mandatory.

This course is delivered monthly by the university Web Team and the Vice-Chancellor's Office, and covers:

1) Key online content management competencies.
2) Key information and training on information management and data protection.

A short pass/fail test on both modules is carried out at the end of this course, which individuals must pass if they are to be considered a potential approver.

Content approver privileges will be revoked by the Digital Services Manager in the event of any of the following;

- A content approver fails to attend a mandatory training course.
- A content approver does not pass the annual refresher training course.
- A content approver cannot demonstrate adequate competencies required to safely carry out the role.

Any revocation of privileges will be formally notified to the relevant FOO or Director.

Public vs internal online content

All online content on the university website fits broadly into one of three categories, outlined in the table below. The type of content should always determine the way in which it is shared.

Content Type	Description	Online Presence
Public facing content	Content either explicitly for public consumption or internal facing content for which no restriction is necessary	Web page or Document page linked to file
Internal facing content	One which requires a login by **staff and students** (the two audiences cannot currently be distinguished between) *Note, **accepting the risk of internal content** below.*	Web page or Document page and linked file, secured behind a login.
Pointer to internal, offline content	Content the existence of which public or internal audiences need to be aware, but which has failed a risk assessment for hosting online	Web page containing details of document owner or offline location (e.g. shared folder or drive).

Personally Identifiable Information (PII)

By default any personally identifiable information (PII) should never be placed on the website or portal (with one exception below). Where it is considered to be appropriate to place PII content on the website without exception the content approver must discuss the

circumstances with the Information Compliance Manager and submit a Privacy Impact Assessment (PIA) for consideration before publishing any content. If in any doubt as to the classification of content in relation to the Data Protection Act the Information Compliance Manager must be consulted.

PII content can be accessed through the portal only where it is fully authenticated at an individual level via a relevant self-service information system; for example, academic staff accessing the personal tutor system via single sign on.

Public folders

The university accepts that in a limited number of instances staff content creators require public folders on the website within which to place specific files (e.g. RTF or XML files).

Requests for such folders may be logged with the Web Team, who will require Faculty Operating Officer or Director sign-off.

Accepting the risk of internal content

The web is an inherently public medium and, in all instances, content should be assumed as likely to default to such whenever a technical or human error arises.

As a result **all** content posted online should be considered to carry a high-risk of being made public, **regardless** of any technical barriers or settings within the website or elsewhere.

If this is deemed an unacceptable risk then the content should never be placed online.

Reporting an issue

If any staff member feels that this governance has been breached, they can report this to governance-issue@gre.ac.uk. This email will always be routed directly to the Digital Services Manager and the Information Officer who will reply within 1 working day.

Appealing a decision

If any staff member feels that a governance action was unfair or not fully considered, they should raise their concern with the Digital Services Manager who will examine the decision and provide an explanation (where appropriate) of why it was made within 1 working day. If this response is still deemed unsatisfactory a staff member may appeal to the Chief Operating Officer, whose decision is final.

Document control

Document Title	Web Content Governance Policy
Authoring organisation	Information & Library Services
Approving Body	Communications Consultative Group
Published/Circulated to	IT & Library Policy web pages Records Management Policy pages IT Strategy Board Executive Committee
Date of Approval	April 2016
Date of Review	April 2017
Version	1

Appendix 1: Example faculty governance Structure

The diagram below describes an appropriate implementation of the approval / workflow mechanisms detailed in this governance structure within a university faculty.