**Digital Governance**

**Code of Practice**

1. Digital Governance – Editorial & Content Guidelines

* 1. Editorial Best Practice

* + 1. Web editors must be familiar with and follow the digital standards and guidelines as described in Queen’s University Belfast - Digital Content Standards and Guidelines
		2. Delivery of Microsoft Office documents from public-facing websites is strongly discouraged.
		3. Only University-approved Web Editors who operate according to Queen’s University Digital Content Policy can publish content within the core website.
		4. The University will provide new and existing Web Editors and Managers with training in the Digital Content Policy and its supporting standards and guidelines.
		5. Web Editors must only create content for websites which are within their area of responsibility and areas that they have been granted permission to edit.
		6. Content must be written, structured and presented to support user tasks and needs. User segments of the University web presence include prospective students, influencers of prospective students (such as parents and careers counsellors), current students, alumni and graduates, staff, agents, partners, Government and media.
		7. Content must serve both international and domestic audiences where appropriate.
		8. Web Editors must ensure that content does not duplicate or contradict copy written on other areas of the University’s digital channels.
		9. Web Editors must ensure that content is created in line with the correct style guide and brand guidelines for their area of responsibility.
		10. When preparing content, Web Editors must follow the metadata schema endorsed by the Metadata / Audience standards and guidelines.
		11. All Web Editors should ensure that content is written in a style that is appropriate for the page's intended audience.
		12. It is the responsibility of Web Editors / content owners to ensure that content is kept upto-date, and archive out-of-date information regularly.
		13. It is the responsibility of Web Editors / content owners to ensure that content metadata is added and that content is prepared following our audience / metadata structure and search engine optimisation guidelines so that users can find it easily, and so their content ranks well in search engines.
		14. It is the responsibility of all parties storing materials on University websites to ensure that such material does not violate other parties' proprietary rights and does not otherwise violate law or applicable University intellectual property / copyright standards and guidelines.

* 1. Content Lifecycle

* + 1. Web Editors are responsible for ensuring that all content within their area of responsibility remains up-to-date, accurate and consistent throughout its life-cycle.
		2. Web Editors must ensure that content is kept up-to-date, and remove or archive out-ofdate information regularly.
		3. When managing and maintaining content, Web Editors must follow the stages described in the Content Lifecycle Guidelines (Planning, Development, Management, Deployment, Revision and Removal)
		4. Web Editors must consider the resource implications associated with managing and maintaining large numbers of web pages.
		5. Web Editors must prioritise important content and focus on operating within University / Area of Responsibility constraints.
		6. Web Editors should maintain a full content calendar to help manage and plan content activity throughout the academic year.
		7. Web Editors should plan content around key University / Area of Responsibility events or important dates and make sure that content is ready in plenty of time to publish.
		8. Appropriate authorisation must occur prior to publishing, including authorisation from the content owner.
		9. The University reserves the right to remove, archive and/or deny access to content that does not meet the criteria outlined in this policy document. Reasonable efforts to contact the unit’s Web Editor / site owner and/or the individual responsible for creating and maintaining the content in such cases will be made; however, content may be removed without notice if required by the severity of the policy violation.

* 1. User Management

* + 1. Content authors, editors and owners must have the level of privileges required to carry out content development of relevant business areas. The level and scope of privileges must be agreed by the Head of the business area.
		2. It is the business owner’s responsibility to ensure that users are added, modified or removed as required.

* 1. Training

* + 1. It is the Web Editor / content owners’ responsibility to ensure that all content contributors are adequately trained in the use of the relevant systems required to create, publish, measure and maintain content within there are of responsibility.
		2. Prospective CMS authors must attend a briefing session covering the key concepts of creating content for the Queen’s Digital Channel before being given access to the system. Existing authors should attend refresher sessions relating to changes in legislation, University policies or changes in the underlying system.
		3. Where non-core systems are used, it is the business owner’s responsibility to ensure that adequate procedure documents and user guides are available for the relevant systems required to create, publish, measure and maintain content within their area of responsibility.

* 1. Accessibility

* + 1. The University has a legal requirement to present accessible web content.
		2. Queen’s is committed to making the information and resources provided via its website accessible to all users. We aim to be standards compliant and follow general principles of usability in order to help all visitors to this website.
		3. Digital pages must, where possible, comply with guidelines on accessibility issued by the World Wide Digital Consortium (W3C) Digital Accessibility Initiative in order to assist in compliance with the Special Educational Needs and Disability Act 2001, Disability Discrimination Act 1995, and Section 75 of the NI Act 1998.
		4. The University acknowledges that this is an ongoing process and are working with information providers across the University to ensure that all future web pages are compliant with accessibility guidelines. In order to ensure no user is disadvantaged while this work is carried out, the University intends to respond to all requests for assistance with accessibility by either altering the necessary content as soon as possible, or, if requested, by providing the information in an alternative format at no cost, within a reasonable timeframe.
		5. It is the responsibility of the Web Editor / content owner to provide alternative formats.
		6. University websites must provide appropriate channels of communication for feedback about accessibility.
		7. Accessibility awareness must be included in the general training provided to all new CMS or non-core system authors, and must be included in refresher courses where appropriate.
		8. Accessibility analysis tools will be used to check content compliance.
		9. Further information on accessibility is available from the disability.office@qub.ac.uk)

* 1. Social Media

* + 1. All staff engaging in social media activity that by its nature of content or look could be affiliated with Queen’s must comply with the University’s Social Media Policy for Staff and associated standards and guidelines.
		2. In accordance with Queen’s University Social Media Policies, all University affiliated social media accounts must be registered. This includes any site that by its nature of content or look could be affiliated with Queen’s.
		3. The University reserves the right to monitor University affiliated social media sites and, where necessary, request the removal of sites or content that that are not in accordance with the Social Media Policy for Staff.
		4. The University operates a number of core social media channels which are managed by the Social Media Manager. Content owners can suggest / request items to be included within core social media channel posts. Requests should be made through Queen's Social Media Manager – requests will be considered in relation to core channel content plans and strategy.
		5. Management of the social media channels will be the responsibility of the official account administrator(s), however, where an account is not being managed appropriately, it will be marked for official review. If, after advice has been given and an allotted period for change passes, the account continues to not meet Queen’s standards, the account administrator(s) will be required to deactivate the account.
		6. For further advice on the use of social media at Queens, please contact socialmedia@qub.ac.uk or the Social Media Manager.

* 1. Analytics

* + 1. Three main web analysis tools are used at Queen’s, Google Analytics, Piwik Analytics and Awstats. They are used to monitor the traffic to the site, to collect information about how users are using the site and to produce reports for business and marketing purposes. The information gathered is not used to identify individual users.
		2. All core website pages must include the central Google Tag Manager and relevant code snippets to allow website usage to be tracked, measured and reported through the central Google Tag Manager account.
		3. It is the Web Editor / content owners’ responsibility to ensure web traffic analysis is conducted periodically for the purposes of reporting KPIs, assessing website effectiveness and driving continuous improvement in usability and accessibility.

1. Digital Governance – User Experience & Design

* + 1. When planning new websites, redesigning existing websites or making significant changes to website structures, business units must seek guidance from the central Digital Manager and Faculty Digital Marketing Officer relating to design and user experience best practice techniques and how to support the business goals of the University by optimising the online experience for our key audiences.
		2. Business units must adhere to the core University brand and digital guidelines
		3. Business units must ensure that all new websites are built to standards that support coding and accessibility best-practices.
		4. Business units must work on custom design solutions only as a last option and where a clear business need has been established.

1. Digital Governance – Network & Infrastructure

All core Digital Channel services will be underpinned by “*Strategic Systems*” supported by the relevant support agency. The following sections outline the conditions that strategic systems must operate within.

* 1. Hosting Platforms

* + 1. The principal hosting platforms for the publishing of online services shall consist of:

* + - 1. Linux (usually the latest recommended release of CentOS)
			2. Apache web server
			3. MySQL or MariaDB
			4. PHP

* + 1. If there is sufficient demand, an alternative on line service hosting platforms based on Windows Server, IIS and Microsoft SQL Server will be implemented.

* 1. Security

* + 1. All strategic systems must be housed in a secure physical environment, with access restricted to nominated personnel.
		2. All strategic systems must reside behind the University’s firewall systems. Where specific services need to be provided off-campus, the technical arrangements must be agreed with the Information Services’ Security Group.
		3. Access to systems will be restricted to nominated users. This may be at an institutional, departmental or functional level.
		4. Sensitive systems should have a secondary level of authentication.
		5. All strategic systems must be implemented such that they are capable of withstanding any attempt to gain access other than for the purpose(s) for which the system is deployed. This includes following best practice across the sector, and recommendations from the supplier of the system.
		6. Sensitive data should be encrypted when stored and transported between systems.
		7. Access to any and all data that is not specifically intended to be accessed by members of the general public must, as a minimum, be secured by requiring the user to be authenticated against the University’s Active Directory. In particular, the use of htaccess files to provide ad-hoc access control (whether on the basis of the user’s identity or the user’s location) for data that is stored on otherwise public systems is deprecated. Where such arrangements currently exist they should be reviewed, with a view to being eliminated, as a matter of urgency.
		8. The holding and use of data within system must be carried out in line with the University’s Data Protection Policy.
		9. Users accessing the system must abide by the University’s security policies.
		10. Any use of cloud based platforms must ensure a level of security required for the sensitivity of the data in question.
		11. Any breaches in security must be reported immediately to the Information Services’ Security Group.
		12. The security of any strategic system may be audited by the Information Services’ Security Group.

* 1. Performance

* + 1. All strategic system architectures must be built in line with best practice across the sector, and where appropriate, recommendations from the supplier. This should include built in tolerance for growth in service demand.
		2. New and upgraded strategic systems should have an appropriate level of stress testing before entering live service.
		3. Strategic systems should be monitored to ensure an appropriate level of service. This should include the use of active triggers to highlight potential issues.
		4. Management tasks such as backups and security testing must be carried out in a manner that minimises any negative impact on performance.
		5. Where possible, all strategic systems should be built on a technical environment with a multi-layer architecture that can facilitate growth in service.
		6. Strategic system performance should be included in Information Services Status Pages, and reported on a regular basis.
		7. New and upgraded systems should be designed to provide a “mobile first” policy that provides a high level of performance across all common platforms.
		8. System Managers should ensure that all systems are up to data with latest software updates as appropriate. Users should be given appropriate notice of any system downtime or at risk periods.

* 1. Disaster Recovery and Business Continuity

* + 1. All strategic systems must be implemented such that there is no interruption to the service in the event of failure of a single server (or the environment that is supporting that server). This will require the use of redundancy technologies and/or multiple physical locations. This may include the use of Cloud technologies.
		2. All strategic systems must have a published Disaster Recovery Plan that highlights the impact of loss of service, and details measures to restore availability of the service. This plan shall be reviewed, tested and re-approved on a regular basis.
		3. All strategic systems must have their data, and system backed up on a regular basis. Backup may be to the Cloud. Regular restores should be carried out to check the integrity of the backups.
		4. System updates should be tested before being introduced to live service.
		5. All new systems must publish an approved Disaster Recovery and Backup Plan before going live.

* 1. Environment

* + 1. All strategic systems must be housed in a secure physical environment, with access restricted to authorised personnel.
		2. Physical environments must provide appropriate levels of networking and power.
		3. Physical environments must provide monitored climate control. Where possible, they should permit generated heat to be re-used elsewhere in order to assist with the University’s sustainability policies.
		4. All strategic systems should be built on a technical environment designed to co-exist with the University’s existing network and security systems. This includes co-existing with University firewall protocols.
		5. All strategic systems should be built on a technical environment with a multi-layer architecture that can facilitate growth in service.
		6. All strategic systems should support an enterprise architecture concept of secure data sharing. In particular, supplying data to support core online services.
		7. All technical environments must be monitored actively to ensure system health and performance.
		8. Technical environments should seek to use the optimum combination of on premise and Cloud based platforms.
		9. All technical environment architectures, performance metrics, Disaster Recovery and Backup plans should be published.

* 1. Non-core / satellite sites

* + 1. Organisational units other than Information Services may host non-core systems where specific functionality is required. In such cases they must follow the guidelines set out in “Hosting Departmental Systems” (still to be produced). Specifically:
			- 1. All non-core /satellite systems must be registered with, and approved by, Information Services.
				2. Each such system must have two nominated systems Administrators who are each under the managerial control of the unit for whose benefit the system is being operated.
				3. Each such system shall comply with the security requirements that are set out in section 3.2 Security above. Prior to going live, each such system shall be subject to an initial security audit which shall be performed by, or on behalf of, Information Services’ Security Group.
				4. Each such system shall comply with the requirements for Disaster Recovery planning as set out in section 3.4 Disaster Recovery and Business Continuity above. The Disaster Recovery Plan shall highlight the impact of loss of service both to the unit for whose benefit the system is being operated and, if relevant, to the University as a whole.
				5. Each such system shall comply, as appropriate to its purpose and scope of operation, with the environmental standards set out in section 3.5 Environment above. Deviations from clauses 3.5(i) to 3.5(iv) of section 3.5 shall be permitted only in exceptional circumstances.

1. Digital Governance – Development & New Sites

* 1. New Websites Site Initiation

* + 1. Proposals to create new websites must be approved in advance of site publishing. This also applies to major redesigns of existing websites.
		2. Proposal will include: business goals, measures of success, target audiences, resources required, ownership (both business and technical), lifecycle plan, domain request and also an acknowledgement of the web standards to be met.
		3. Proposals must be submitted to the Digital Operations Group.
		4. The Digital Operations Group will advise business owners / requestors of decision on development lifecycle approach through from system design, planning, development and maintenance in a business as usual environment.
		5. Requests for domain names will be reviewed by the Digital Operations Group. Requests for Group sub-domains will be reviewed jointly by Queen’s University Digital Management Group and Information Services.
		6. For non-qub.ac.uk domains, the website owner is responsible for registering or renewing the website domain and informing the Digital Operations Group of any changes to the non-qub.ac.uk hosted website domain’s registration status.
		7. A domain name may be deleted if a website is being deleted or archived or the domain no longer forms part of the University’s domain optimisation strategy. Information Services networks will consult with content owners in accordance with the deleting websites standards and guidelines. Approval of sub-domains will be subject to the conditions set out in section 4.2 Domains and Subdomains.
		8. Any domain, sub-domain or any relating URL must not be used on any material before it is approved.
		9. All URLs (Uniform Resource Locator) should comply with the University URL standards and guidelines. This includes short URLs created for marketing or social sharing purposes.
		10. All new University websites must meet level AA of the Web Content Accessibility Guidelines version 2.0 as standard. This includes, but is not limited to:
			- 1. core websites
				2. website sections,
				3. Academic Schools, Faculties and Research Centres
				4. non-core Queen’s websites where the University is a partner in the initiative. e) related sites
		11. Social media websites must be created and maintained with reference to University Social Media Policies and associated standards and guidelines.

* 1. Domains and Subdomains

* + 1. The primary role of subdomains will be to provide access to core service areas, and internal zones that do not link naturally to the core public business of the University.
		2. Subdomains will be used to define core Queen’s University system services, including, but not limited to:
			- 1. email.qub.ac.uk
				2. qol.qub.ac.uk
				3. search.qub.ac.uk
				4. cms.qub.ac.uk
				5. qsis.qub.ac.uk
				6. archive.qub.ac.uk
				7. intranet.qub.ac.uk
		3. Domains may also be used to promote global initiatives as recognised by the Digital Channel Board. For example Global Research Institutes.
		4. Existing subdomains will be reviewed, and where possible non-compliant subdomains will be removed, or phased out over time.

* 1. URL Structure

* + 1. The top level URL structure will be used to reflect core University areas. This includes, but not limited to:
			- 1. Schools and Departments
				2. Research Institutes
				3. Research Centres
				4. External Services (as approved by the Digital Board).

* + 1. In the event that an organisational unit that has a ‘top level’ URL is either re-named or merged with another unit, the original top-level URL shall be disposed of as follows:

* + - * 1. If the unit is being re-named then a new top-level URL reflecting the new name shall be created and all content that was accessible via the original URL will be moved to reside under the new URL.
				2. If the unit is being merged into a unit that already has a ‘top level’ URL then all content that was accessible via the original URL will be moved to reside under the URL of the unit with which it is being merged.
				3. In either case the URL that has been ‘vacated’ shall be populated with a single landing page which will inform visitors that the unit has moved, cite the new URL and encourage visitors to update any relevant bookmarks.
				4. There shall be no automatic redirection from ‘old’ URLs to corresponding ‘new’ URLs nor will URLs be re-written so as to give the impression that the ‘old’ URL is still in use.

* + 1. Short-form URLs shall be provided subject to the following conditions:

* + - * 1. All short-form URLs shall be used to provide a shortcut via re-direction. The URL that appears in the user’s browser when the page has loaded will be the full, native URL of the page without any rewrites.
				2. Requests for either a short-form URL that is not provided by go.qub.ac.uk or a short-form URL that is allocated by go.qub.ac.uk and consists of anything other than a randomly allocated sequence of characters shall be subject to prior approval by (insert approving authority here).

1. Implementation, Monitoring and Remediation

* 1. Implementation

* + 1. This Policy is supported by a comprehensive suite of practical standards and guidelines documents that define good practise for University digital content contributors.

* 1. Monitoring

 (i)

(ii) The University reserves the right to monitor University affiliated websites and social media sites for compliance with this Policy.

* 1. Remediation

* + 1. We want to help people in the first instance to correct gaps in Policy compliance through providing practical advice and support and working collaboratively to support stakeholders in meeting our digital standards.
		2. It is the business owner’s responsibility to ensure that any required remedial action is actioned, implemented and completed.
		3. The University reserves the right to act on any information obtained through our digital channel monitoring, if it indicates that a user is in breach of University policies or the law.
		4. The University reserves the right, where necessary, to request the removal of sites or content that that are not in accordance with this Policy

1. Further Information

Further information on this policy is available from Strategic Marketing and Communications, on request.