Derby City Council

Website Standards & Development Guide (WSDG)

Technical requirements

Version Control

Version	Date	Author	Amendment history
Draft A	25/07/2012	Adam Radford	Modified original Website Standard and Development Guide to create three separate documents. Extensively updated and re-written.
Draft B	26/07/2012	Adam Radford	Modifications following internal review.
Issue 1.0	27/07/2012	Adam Radford	First release.
Issue 1.1	23/05/2013	Kevin Hutchby	Link to Geospatial data standards included
Issue 1.2	27/11/2013	John Crowther	Added section 9 about URL standards
Issue 1.3	11/02/2014	John Crowther	Updated Media advice section 5.4
Issue 1.31	13/02/2014	John Crowther	Minor revision to section 9.1 (domain names)
Issue 1.32	02/04/2014	Kevin Hutchby	Minor revision to fix a section link
Issue 1.33	30/04/2014	John Crowther	Minor corrections to layout and introduction text
Issue 1.4	14/05/2014	Adam Radford	Added QR code and URL shortener sections.
Issue 1.41	23/06/2014	John Crowther	Moved SSL advice into Section 8
Issue 1.5	30/07/2015	John Crowther	Rewrite of Flash; Certificates; Browser compatibility and defensive registration. Addition of mobile device compatibility and https by default.

Version	Date	Author	Amendment history
Issue 1.6	07/08/2015	John Crowther	Updated domain registration and Google Analytics advice.
Issue 1.7	01/07/2016	Kevin Hutchby, John Crowther, Adam Radford	Accessibility requirements updated. Change of section orders. Section and content consolidation. Removal of Security requirements into separate document. General simplification of guidance.
Issue 1.8	24/02/2017	Adam Radford	Extensive review and merge of security requirements document. Simplification and removal of duplication.
Issue 1.9	07/03/2017	Adam Radford	Added Privacy and Electronic Communication Regulations (PECR) references for cookies.

Related Documents

Title
Website Standards and Development Guide – Visual Requirements

Comments and feedback

Please refer any feedback to the Derby City Council Web Team via webteam@derby.gov.uk.

Contents

1. Overview

The document forms part of the Derby City Council Website Standards and Development Guide (WSDG).

These standards will form part of any website or web application development contract with the Council. Vendors may be asked to provide evidence of successful testing against this standards document.

Vendors should note that:

- Derby City Council has a responsibility to provide its services in line with the Equality Act 2010 (EA).
- Our standards include adherence to World Wide Web Consortium (W3C) accessibility guidelines.
- The Council undertakes regular testing against both Payment Card Industry (PCI) and Public Sector Network (PSN) standards.
- All .gov.uk domains and sub-domains need to following the Government Digital Service (GDS) guidance for “Local government: naming and registering websites”.

The latest Website Standards and Development guide can be found at: www.derby.gov.uk/site-info/web-development-guide/.

2. Application/Web pages

Key points:

- Valid and semantic HTML mark-up must be used.
- Pages should validate against the W3C validator service at http://validator.w3.org/
- Content and styles must be separated.
- Valid CSS must be used for layout.
- There must be full adherence to W3C WAI accessibility standards.
- The use of HTTPS for all websites and applications.

The Council reserves the right to turn off services where they believe there is a significant risk – either technical, reputational or legal (EA) – by failure to meet our web standards.

2.1. URLs and file naming

Wherever possible, files and folders should have a meaningful name and relate to the content inside (irrespective of whether the file is html, an image, CSS or other).

Filenames must be lowercase with the title of the document separated by hyphens, not spaces or underscores (e.g. council-tax-application-form.pdf).

The use of IDs and parameters within URLs should be avoided wherever possible.

Section 4 discusses Domains and URLs in more detail.

2.2. HTML Standards

HTML5 is highly recommended for all websites/applications.

Other strict Document Type Declarations (DOCTYPES) can be used for legacy websites/application developments.

All pages must validate against the DOCTYPE used. We recommend using the W3C validator service at http://validator.w3.org/.

All HTML should be logical and semantic. For example, order of header tags, paragraphs, ordered and unordered lists, blockquotes to be used appropriately.

As a minimum, the following metadata must be coded into the <head> sections of all pages:

- Title
- Description
- Keywords

2.3. CSS Standards

All CSS files must be semantic and validate to W3C standards. We recommend using the W3C validator at https://jigsaw.w3.org/css-validator/

Inline styling should not be used unless absolutely required.

CSS 'hacks' (to satisfy non-standards-compliant web browsers) should be kept to a minimum and should be in separate CSS files. They should also be clearly commented to indicate which browser issue is being addressed.

Pages must be viewable in a logical order without CSS.

Stylesheets to be provided:

- screen (mandatory)
- print (mandatory)
- handheld (optional)

2.4. Device types

Public facing websites/applications should be designed with **all** device types in mind.

Our preference is for Responsive Design techniques to be employed.

2.5. Page Weight

Homepage and landing pages must be kept as lightweight as possible.

Recommendations:

- Use Google Page Speed (http://code.google.com/speed/page-speed/) for evaluating page performance.
- Where appropriate: combine and compress/minify stylesheets and JavaScript
- Enable suitable web server compression (for example, gzip or deflate).
- Optimise/resize images appropriately to balance page weight/image quality

2.6. Browser compliance

Websites must work (in non-quirks mode) in the following browsers (both desktop and mobile versions):

- Internet Explorer/Microsoft Edge (current supported versions)
- Chrome (versions 12 months old or less)
- Firefox (versions 12 months old or less)
- Opera (versions 12 months old or less)
- Safari (current supported versions)

For older browsers, we expect graceful degradation of a website rather than a minimum level of browser to be required.

2.7. Page and content caching

Cache-Control and Expiry HTTP headers should be used on all applications and websites to prevent excessive (and uncontrolled) browser caching.

We recommend considering that flat content, images, JavaScript and CSS files could can be set to cache for different times, depending upon the frequency of change.

For applications showing information specific to a user's session or login and for forms, webpages themselves should usually be set to so that they expire immediately, or so that caching is disabled.

2.8. JavaScript and AJAX

JavaScript and AJAX are acceptable as long as they do not break W3C Accessibility for Priority 1 and Priority 2 guidelines.

Fall-back functionality/content must be provided for when users disable JavaScript in their browser, or for browsers with limited/no JavaScript functionality. We expect a graceful degradation to the user experience in scenarios like this.

2.9. Inline Frames

The use of iframes within pages is discouraged.

However, it is recognised that for certain types of integration with third party services, iframes are the only option.

Where iframes are used, the fully rendered page must be able to be read accurately and completely by assistive technologies (for example, screen readers).

2.10. Tables

HTML Tables must only be used for presenting tabular data, not for layouts.

2.11. Hyperlinks

Links to websites must open in the same window/tab (unless opening in an alternate window or tab is required for specific functional reasons).

Any text used as a hyperlink must make sense when read out of context, accurately describing where the link goes to. Link texts such as “more”, “click here” or “next” must never be used as link texts for reasons of accessibility.

2.12. Site Analytics

All websites should utilise traffic analytics, in order to provide the Council with meaningful usage statistics.

The Council prefers the use of Google Analytics (GA), however other analytics tools can be used if absolutely necessary.

The Council wishes to retain control of the generated analytics data, therefore websites must use a GA tracking ID provided by the Council itself. This can be provided by the Council’s Web Team.

Access to analytics data can be provided to relevant 3rd parties by the Council, upon request.

If a tool other than GA is used, access to data must be provided to the Council.

2.13. Images

Use of images for text is strongly discouraged. In such cases (as per W3C standards), the ALT and TITLE attributes **must** be used to comply with accessibility and coding standards.

2.14. Banners and Logos

The site homepage must be linked to from the banner/logo on each page.

It is desirable to identify all Council websites/microsites by featuring the Derby City Council logo in the top banner unless design constraints disallow this - in which case the logo should appear in the site footer.

2.15. Sitemap, Terms & Conditions, Privacy Policy and Accessibility

A Site Map, Terms and Conditions of use, Privacy Policy and Accessibility statement must all be provided. These should be presented as separate content pages or downloads.

Privacy Policies should be referenced in text whenever forms request personal information from a visitor.

Privacy Policies should detail the organisation's data protection policy and describe the site's use of cookies in line with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (see http://www.derby.gov.uk/site-info/privacy-statement/).

The PECR states *"You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the users' consent. Consent can be implied, but must be knowingly given"*.

Section 2.18 details the use of cookies and session state.

2.16. Search

Search functionality should be provided on dynamic data driven sites.

An in-house search appliance can be used where an application requires a search facility. Requirements for search functionality should be discussed with the Council's Web Team.

2.17. Accessibility

Derby City Council has a responsibility to provide its services in line with the Equality Act 2010 (http://www.legislation.gov.uk/ukpga/2010/15/contents)

There must be full adherence to WAI accessibility standards: All WCAG 2.0 Level 'A' and Level 'AA' (Priority 1 and 2) requirements must be met (https://www.w3.org/TR/WCAG20/).

2.17.1. Access Keys

If Access Keys are used then the following must be adhered to:

S – Skip navigation

1 – Home page

2 – What's new

3 – Site map

4 – Search

5 – Frequently Asked Questions (FAQ)

6 – Help

7 – Complaints procedure

8 – Terms and conditions

9 – Feedback form

0 – Access key details

2.18. Cookies and session state

Session based cookies should be used in preference to persistent client-side cookies wherever possible. Where persistent client-side cookies are used, a short expiry date should be set that is appropriate for the application's needs.

Cookies should never contain sensitive or editable data. The use of encrypting data within cookies (such as for logon tokens) should be kept to a minimum. Public standards should always be followed rather than in-house cryptography.

Session information should never be sent to or from the client in session objects, hidden fields or within query string parameters.

2.19. Security certificates and HTTPS

2.19.1. HTTPS by default

It is the Council's ambition to provide all online services using HTTPS by default. It is therefore recommended that HTTPS is used for all content.

If personal or sensitive data is transmitted then the site **must** use HTTPS.

Redirection from HTTP to HTTPS should be put in place to ensure visitor attempts to use HTTP are handled elegantly.

If the vendor manages the server publishing the online service, regular testing should be carried out to ensure that security certificates and service are securely configured.

For example, the website https://www.ssllabs.com/ssltest/ provides a thorough analysis of internet facing websites. The Council recommends that servers should obtain a grade “A” in such tests.

2.19.2. Security certificates

For sites residing on Council owned and managed domains, all security certificates **must** be purchased by the Council’s ICT department and be registered in the name of Derby City Council (or the relevant Council body) rather than a vendor/supplier.

Requests for certificate purchases should be sent to the Council’s web team.

This includes websites developed by third-party developers, when the Council owns the domain name. This is to ensure that the Council are able to successfully validate certificate requests with the Certificate Authority (CA).

If an application is hosted on a supplier’s domain that is completely owned and managed by the supplier (for example Software as a Service), then it is acceptable for security certificates to be obtained and managed by the supplier.

The Council uses Organisational Validation (OV) certificates by default. Domain validation (DV) certificates should not be used.

Certificates must:

- have 256 bit encryption.
- have a 2048 bit key.
- be recognised by all browsers listed in section 2.6.

Under no circumstances should self-signed certificates be used. The Council has internal PKI servers that should be used whenever an internal only application requires HTTPS.

3. Media

3.1. Flash/Silverlight

Adobe Flash and Microsoft Silverlight should **not** be used on newly developed web applications.

HTML5 can be used to provide similar functionality in most cases.

3.2. PDF files

PDF files must be authored with accessibility in mind and must be correctly tagged with a logical reading order.

As a minimum, the following PDF document properties must be set

- 'title field' must reflect the document title and not the filename.
- 'author field' should contain the organisation name.

For further information, see http://www.adobe.com/accessibility/.

3.3. Other File Formats

Where possible, use PDF and CSV in preference to Word, Excel, PowerPoint and other proprietary file formats.

3.4. Video and audio content

Video and audio content must work on all modern browsers.

The Council has Vimeo Pro account which allows us to control branding, player design and remove adverts. Vimeo allows a video to be publically listed, or set to private.

Audio should also be presented using the same techniques as video presentation – to allow for improved streaming over the HTML5 `<audio>` tag.

If a different online streaming service such as YouTube is required for other justifiable reasons campaigns, then this is acceptable. The Council has an official YouTube channel that can be used for this purpose.

If a video has been produced for and remains the intellectual property of the Council, we require the best quality version to be provided to the Council for archival storage.

Our advice about which service to use is summarised in the table below:

Purpose/Platform	Vimeo Pro	Other service (such as YouTube)
General video on external website (for public consumption)	Yes	Yes (with DCC permission)
Commercial video on any website	Yes (video will be marked as private)	Yes (with DCC permission)
General video on internal site (for internal use only – For example, the Council's intranet) *	Yes (video will be marked as private)	No
Confidential video on internal website	No	No
Audio on external site or internal site	No	Yes (with permission)
Confidential audio on internal site	No	No

***** Note: media designed for internal use that is hosted privately on Vimeo can viewed by others if the video URL is obtained. If intranet content is confidential then Vimeo must not be used.

Please contact the Council's Web Team for advice about using any of these platforms.

3.4.1. Video accessibility

Closed captions or a transcript should be provided wherever possible.

If a new video or recording is being created then consider this part of the production effort.

Closed captions are more preferable to transcripts as these can be selected by the user when appropriate. If a transcript is used, it should be provided on the web page, adjacent to embedded media.

Do not "burn in" closed captions into a video. Provide the subtitle file to Vimeo or YouTube. It will be then be selectable in the video player.

Further advice about creating closed captions can be obtained from the Council's Web Team.

3.5. Geospatial data

Where map services are used on websites, standards must conform to those set out by the Open Geospatial Consortium: http://www.opengeospatial.org/standards/is.

For more information, please contain the Council's Geographic Information Team at gis@derby.gov.uk.

4. Domains and URLs

4.1. Domain names and registration

All .gov.uk domains and sub-domains need to follow the Government Digital Service (GDS) guidance for "Local government: naming and registering websites" which can be found at https://www.gov.uk/government/publications/naming-and-registering-government-websites/local-government-naming-and-registering-websites).

All domain names **must** be purchased by the Council's ICT Department (This includes domains for websites developed by third-party developers).

Requests for domain name purchases should be sent to the Council's Web Team.

When purchasing domain names, we will check and register the following (primary/secondary domains) **as a minimum:**

- <name>.co.uk
- <name>.com
- <name>.net
- <name>.org
- <name>.org.uk
- <name>.uk

Once a website is decommissioned, the primary domain **must** be continued to be registered for a minimum of 5 years.

The Council's Web Team will configure any secondary domains so that browsers are forwarded to the primary domain.

4.2. Use of Directories and subdomains

The top level directory (e.g. derby.gov.uk/ or cmis.derby.gov.uk/) **must** always contain meaningful content or redirect appropriately.

Holding pages or "file not found" messages are unacceptable.

For promoting URLs: always use derby.gov.uk/<service> rather than the subdomain <service>.derby.gov.uk.

The prefixes "http://", "https://" and "www." should not be used when promoting URLs. HTTP redirects should be used be redirect visitors to the appropriate URL.

4.3. URL Shortening services

Wherever practical, friendly URLs (such as derby.gov.uk/planning) should be used rather than third party URL shortening services (such as bit.ly and goo.gl). The Web Team can assist in creating friendly URLs on the derby.gov.uk domain that redirect to other sub-domains and websites.

However, where a large number of shorter URLs are required, tracking is needed, or extremely short URL use is required, a public URL shortening service can be used (recommended: http://goo.gl).

4.4. QR Codes

QR codes provide an easy way for members of the public to access URLs without having to type the URL.

QR code that links to derby.gov.uk via goo.gl URL shortening service

We recommend that QR codes are generated using the http://goo.gl URL shortening service.

5. Website Security

5.1. Application security

The supplier **must** ensure:

- The application is tested to and meets Level 2 of the current OWASP Application Security Standard, found at:

  https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

  Note: Developers may find the OWASP Testing Guide useful, which covers the procedures and tools for testing the security of applications:

  http://www.owasp.org/index.php/Category:OWASP_Testing_Project

- Applications and server environments are secured to withstand Payment Card Industry (PCI) and Public Sector Network (PSN) checks. The Council regularly undertakes both. Should be application or server environment fail such a check, the vendor will perform remediation action in a timely manner

5.2. Web server/file security

The supplier must ensure:

- There is a robust patch management process in place for assessing, identifying, evaluating and deploying latest patch releases.
- Any unused services, files and applications are removed from live servers.
- The web server account has:
  - Only read access permissions to the web folder, unless write access is absolutely necessary.
  - Has no or minimal permissions to other folders, drives or computers.
  - No read or delete permissions to the server log files. The web server log files are located on a separate drive, partition or machine.
- Database connections only provide the minimum user rights required by the application.

5.3. User authentication

The supplier must ensure:

- Best practice should be followed for the storage of username and password information within databases. Values should be uniquely salted and hashed as a minimum. Public standards should always be followed rather than in-house cryptography.
- IP whitelists are used to restrict access to login and administration pages wherever possible.

5.4. Input validation

The supplier must ensure:

- Form input values are fully validated.
- Form input values are never concatenated into SQL statements without sanitisation (in order to prevent SQL injection attacks). If the programming language supports it, parameterised queries should be used.
- Validation is always handled at the server instead of the client.
- Validation errors are handled elegantly. Users should never see sensitive information, server and environment names or internal error messages.

5.5. Data security and processing

Any application which handles personal or private information **must** comply with the UK Data Protection Act and the Computer Misuse Act.

We follow the Information Commissioner's Office (ICO)'s definition of 'personal data' and 'sensitive personal data'.

The ICO's "definition of personal data" (https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/#personal-data) and ICO's "data protection principles" (https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/) contain useful information in this regard.

Section 2.15 details the use of Privacy policies and PECR regulations.