PERIMETRY RESEARCH

Security barometer of the UK councils

How well do the UK councils protect their websites and e-mail? Passive measurements of the domains of the principal councils of England, Wales, Scotland and Northern Ireland.

November 2026 edition

359
domains with a site of their own, graded

95.5%
enforce DMARC (quarantine or reject)

35.9%
get an A or a B

Perimetry Cloud
perimetry.cloud · Published 14 November 2026

About this report

Perimetry Research publishes studies of how well organisations protect their websites and e-mail, measured with the same passive checks as Perimetry Cloud. This edition covers 366 domains of the UK's principal councils; 366 are active, and the 359 with a site of their own are graded. It names only the authorities that do well; every other figure is an aggregate, and the serious issues were reported privately to the authorities before publication.

Contents

01 Executive summary 3

02 Key findings 4

03 Grades 5

04 Check by check 6

05 By category 8

06 Domains without a site of their own 9

07 Compared with our other studies 10

08 The authorities that get it right 11

09 Serious issues 12

10 Recommendations 13

11 Methodology 14

12 About Perimetry 16

01

Executive summary

359
domains with a site of their own, graded

69
average score out of 100

95.5%
enforce DMARC (quarantine or reject)

35.9%
get an A or a B

Average score of the 359 graded domains: 69 out of 100; median 67.

1. 99.4% of the graded domains publish a DMARC policy and 95.5% enforce it (French local authorities: 32.8%; German local authorities: 41.1%).
2. Websites: 98.1% have a valid certificate, 85.5% send visitors to HTTPS, 57% use HSTS for six months or more.
3. 1.9% of the graded domains are signed with DNSSEC; 11.4% publish a CAA record.
4. 7 active domains have no site of their own; 0% of them do not enforce DMARC.

02

Key findings

99.4% of the graded domains publish a DMARC policy and 95.5% enforce it (French local authorities: 32.8%; German local authorities: 41.1%).

Websites: 98.1% have a valid certificate, 85.5% send visitors to HTTPS, 57% use HSTS for six months or more.

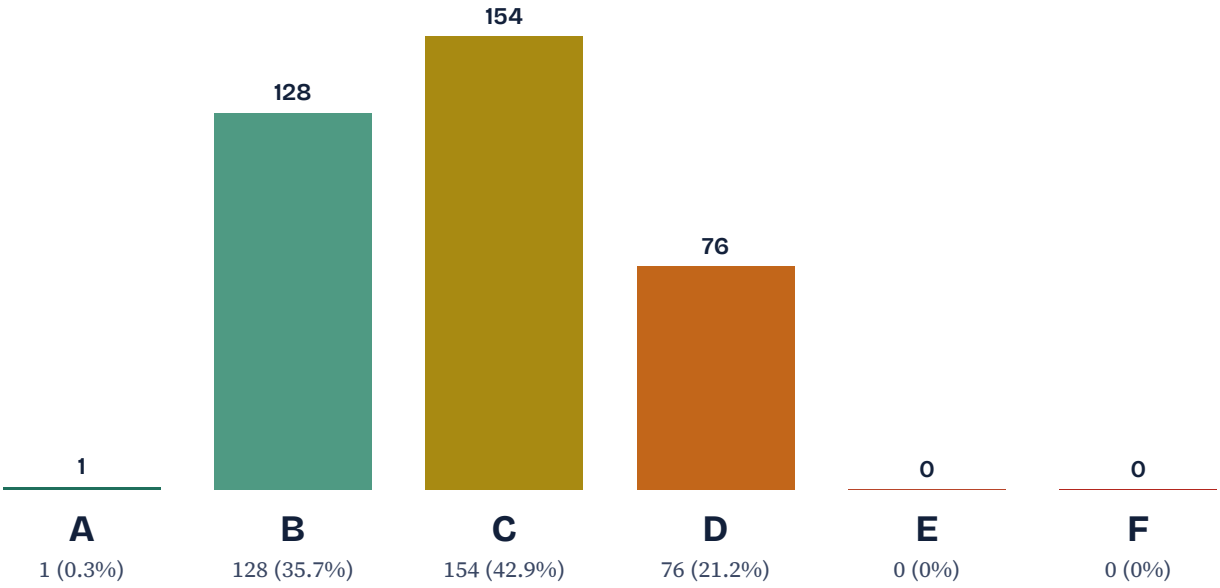
1.9% of the graded domains are signed with DNSSEC; 11.4% publish a CAA record.

7 active domains have no site of their own; 0% of them do not enforce DMARC.

03

Grades

Each domain with a site of its own gets a score: the share of the nine checks that it passes, among those that apply to it (the score of our other studies, without the check on the contact address, which the lists do not give). Grades: A from 90, B from 75, C from 60, D from 40, E from 20, F below.

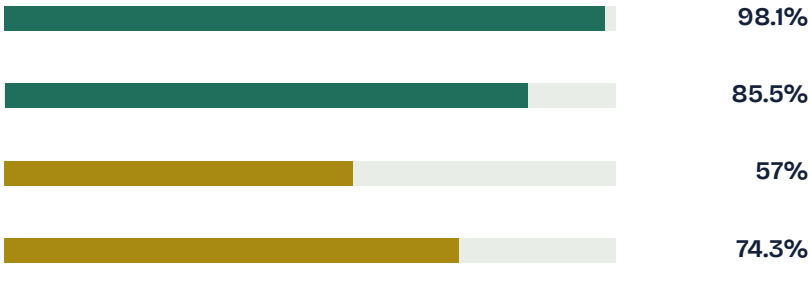


04

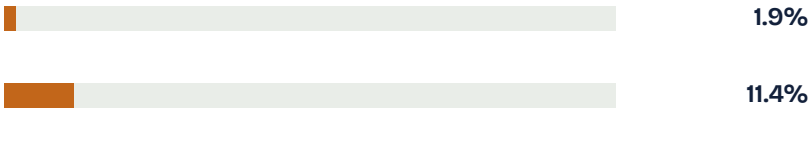
Check by check

Share of the graded domains that pass each check, among those it applies to.

Website



DNS



E-mail



The nine checks	
Website · Valid HTTPS certificate	The site answers over HTTPS with a certificate that is in date, issued for its name, and trusted by browsers.
Website · HTTP sends visitors to HTTPS	Someone who types the address lands on the encrypted site, not on a page anyone on the network can read or alter.
Website · HSTS for six months or more	Browsers remember to use HTTPS only, so the first unencrypted request cannot be hijacked.
Website · Basic protective headers	X-Content-Type-Options: nosniff, and protection against being framed by another site (X-Frame-Options or CSP frame-ancestors).
DNS · DNSSEC	Answers about the domain are signed, so a resolver cannot be fed false addresses for the administration's site or mail.
DNS · CAA record	The domain names the certificate authorities allowed to issue certificates for it.
E-mail · Strict SPF	The domain lists the servers allowed to send its mail and asks receivers to reject or flag the others (-all or ~all).

The nine checks	
E-mail · DMARC record	The domain publishes a DMARC policy, the standard that ties SPF and DKIM to the visible sender.
E-mail · DMARC enforced	The policy is quarantine or reject: messages forged in the administration's name, to citizens for example, go to spam or are refused, not delivered.

05

By category

Categories with fewer than ten graded domains show no figures.

Group	Graded	Average	A or B	DMARC enforced	Median
County councils (England)	21	71	38.1%	95.2%	–
District councils (England)	154	69	33.8%	94.8%	67
Metropolitan borough councils	35	69	28.6%	97.1%	67
Unitary authorities (England)	53	69	39.6%	96.2%	67
London borough councils and the City of London	33	73	51.5%	100%	78
Welsh councils	21	66	23.8%	95.2%	–
Scottish councils	31	69	32.3%	96.8%	67
Northern Ireland councils	11	75	54.5%	81.8%	–

Average



06

Domains without a site of their own

7 active domains have no site of their own: 0 send visitors to another site, 7 are used for mail only. They can still be used to forge e-mail in the authority's name, and are judged on DNS and mail only.



Average score on DNS and mail only: 60 out of 100.

07

Compared with our other studies

The same checks in our other studies (latest editions): share of the graded domains that pass each one. The French local authorities count ten checks, the others nine.

	UK councils	German authorities	French authorities	UK State
Average score	69	62	60	54
Valid HTTPS certificate	98.1%	96.4%	98.7%	67.4%
HTTP sends visitors to HTTPS	85.5%	92%	90.9%	75%
HSTS for six months or more	57%	74.3%	38.8%	42.1%
Basic protective headers	74.3%	68.6%	40.7%	47.8%
DNSSEC	1.9%	15%	25.9%	3.8%
CAA record	11.4%	12.4%	2.6%	4.7%
Strict SPF	100%	88.6%	97.1%	85.6%
DMARC record	99.4%	73.6%	77.8%	84.3%
DMARC enforced	95.5%	41.1%	32.8%	74.6%

08

The authorities that get it right

1 authorities pass every one of the nine checks and have no serious issue.

Authority	Category
Newry, Mourne and Down District Council	Northern Ireland councils

09

Serious issues

2 domains have a serious issue that could be used against them. They are not named in this report or anywhere else: the authorities were told privately before publication.

Expired certificates	2

10

Recommendations

1 **Enforce DMARC**
Most councils already do: the rest should follow, starting with the domains that send no mail.

2 **Turn on HSTS and the protective headers**
HSTS makes browsers remember to use HTTPS only; two headers stop another page from framing the site and the browser from misreading its files.

3 **Sign the domains with DNSSEC**
Almost no council does; the .gov.uk registry supports it.

4 **Check the address without “www”**
Several expired certificates were found on the bare domain while the www site was fine: a visitor who types the short address gets a warning.

5 **Watch it over time**
Certificates expire, providers change, records get lost in a migration. A regular check catches it before residents do.

11

Methodology

Passive checks only

We read what any visitor or mail server can see: public DNS records, the domain registration (RDAP), the TLS certificate, one request for the home page over HTTP (its redirect is read, not followed), and the home page over HTTPS (following its redirects, as a browser would). Nothing else on the site is requested. When a domain publishes an MTA-STS policy, its policy file is read too, as mail servers do.

No port scanning, no subdomain discovery, no login attempts, no forms, no testing for vulnerabilities. The robot is slow on purpose and spreads its requests over several hours.

The robot

It identifies itself as PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). If you run a site it visited and would rather it did not, write to hello@perimetry.cloud and we will leave the domain out of the next editions.

The study of the UK councils

Population: the principal councils in force of mySociety's UK local authority names and codes (CC BY 4.0): the county, district, metropolitan borough, unitary and London borough councils of England, the City of London Corporation, and the councils of Wales, Scotland and Northern Ireland. Parish and town councils, combined authorities and strategic authorities are left out. Each council's website is the one GOV.UK's local authority record gives (Open Government Licence v3.0); two councils that share one domain (shared services) are one domain in the study.

Categories: the council's type in mySociety's list. Everything else follows the study of the French State: inactive domains counted and left out, the main figures on the domains with a site of their own, nine checks, groups of ten graded domains or more, only the councils that pass all nine checks named. A site that answers our robot with an error page (often a filter that turns away data-centre networks) keeps its certificate and redirect checks but is not graded on its headers. The serious issues are reported privately to the council before publication; the study gives their number only.

Good performers only

We name the communes that do well (the honour roll and the best of each size band), never the ones that do badly, and never a commune with a serious issue, whatever its score. Everything else is published as aggregates: by size of commune and by département, where a département with fewer than ten graded communes shows no figures, so that none of them can be singled out.

Website platforms are graded on a sample of up to five communes' sites there: a check counts as passed when most of the sample passes it.

Serious issues are reported privately

Some findings could be used against a commune right away: a domain listed in the official directory that no longer exists (anyone could register it), a registration the registry is deleting, an expired certificate, an SPF record that lets anyone send mail in its name. These are never published. We tell the commune first, quietly, and count them in the study without naming anyone.

Limits

Each edition is a snapshot taken over a few hours. The directory can be out of date or wrong; we use it as published. DKIM keys are looked for on common selectors only, so they are not graded. A site behind a protection service may answer differently to a robot than to a visitor. Mail servers are not tested (STARTTLS needs port 25, which the study's infrastructure cannot reach).

12

About Perimetry

Perimetry is an open source tool that audits the outside of a domain the way anyone on the internet sees it: e-mail authentication, DNS, certificates, mail servers, websites. Perimetry Cloud is its hosted version, with continuous monitoring, alerts and reports, for organisations and the agencies that look after them.

Cite as: Perimetry Research, Security barometer of the UK councils, November 2026. https://perimetry.cloud/research/uk-councils/

You may reuse the figures of this report with a link to the study. Contains data from mySociety (CC BY 4.0) and public sector information licensed under the Open Government Licence v3.0.

Contact: hello@perimetry.cloud

`https://perimetry.cloud/research/uk-councils/`