How UK Councils Look to an External Security and Privacy Scan

A September 2026 baseline of 379 council websites across England, Wales, Scotland and Northern Ireland, written for people who do not work in cyber security

Updated edition, 27 September 2026. Every website was rescanned on 27 September and every figure is from that day. For the first time, every missing score is explained, and faults on councils' own systems are reported.

> **What this report is**
>
> We looked at every council website in our tracked estate from the outside, the way any member of the public could, and recorded what was visible. We did not log in anywhere, try any password, or touch anything inside a council's systems. This report says what we saw, what it means in plain English, and what is worth doing about it.

Sources	Four separately tracked national estates, reported separately: **England 314 websites**, **Wales 22**, **Scotland 32** and **Northern Ireland 11**.
Combined	No website appears in more than one estate, so the four together represent **379 distinct websites**. This was checked rather than assumed.
Evidence	One full rescan, 27 September 2026. **All 379 completed and none failed.** 291 produced an exact score and 62 a floor score, so 353 carry a published figure. 26 produced no score but still produced findings, which are counted throughout, and each of the 26 has been checked individually.
This edition	Supersedes every earlier edition at the same address. Before any comparison was made, the 9 September figures were reproduced exactly from retained scans by the same method; the changes are set out overleaf. **No earlier score contributes to any figure here.**
Limits	Nothing here says any council has been broken into. Nothing here is a legal or compliance judgement. Everything here is what was visible from outside on one day.
Prepared by	Huro Data Technologies Ltd / MyDomainRisk
Date	Assessed 27 September 2026 | this edition 27 September 2026

Research and external assessment: MyDomainRisk | Huro Data Technologies Ltd

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Executive summary

The four things that need attention

1. Stolen staff passwords are circulating for a third of councils. 122 websites, 506 records. These are keys to the council's own systems and the council can take them back today.

2. Three councils run software with a weakness criminals are known to be using now, listed in the public catalogue of weaknesses being exploited in the real world rather than merely recorded somewhere. One sits on an address registered to the council itself, on web server software past the end of its supported life.

3. Twelve councils have a service answering the internet that probably should not be, ten on a database port. Four further cases sit on addresses shared with unrelated organisations and are reported separately. Only four of the twelve have a service actually identified; elsewhere a port answers with nothing identifiable behind it.

4. Sixteen councils have a fault on their own systems that any visitor or mail system would meet. Fourteen advertise an email protection nobody can read. Each has a straightforward fix, in section 12.

Small in count, serious in kind. None of it means a council has been broken into, and every item needs checking privately first. **Three councils have a confirmed lowest-band score**, all in England.

What we found, worst first

What it is, in plain English	Why it matters	Websites
Software weakness known to be exploited now	In the public catalogue of weaknesses criminals are using. 12 more were read from version numbers only.	**3**
A database port answering the internet, at council level	Databases hold records. They belong behind the website, not beside it. Three are confirmed running.	10
Any risky service reachable, at council level	Remote access, file transfer, admin tools. The 10 database ports are inside this 12.	12
The same, on a shared address	Reported separately because no council can close it alone; a weakness there reaches every organisation on the platform.	4
A fault on the council's own systems	Met by every visitor or mail system, not just by us. Each is a configuration change.	16
Cannot stop email being forged in the council's name	Residents act on council emails fast. The cheapest item here to fix.	17
Visitors not forced onto a secure connection	The one a resident could notice. Anything typed in can be read on the way.	27
Staff passwords in criminal collections	Harvested by viruses on individual computers. 506 records.	122
Staff identities exposed on other companies' platforms	Work email addresses used to sign in elsewhere. 949 records.	217
No cookie consent mechanism detected	The regulator actively tests this. Needs checking in a browser.	243

Rows overlap and must never be added. Residents' own account details circulate for 359 councils, 46,948 records, in section 9.

Executive summary, continued

Stolen passwords, and why this is the finding to read twice

What a criminal collection actually is

When a virus infects somebody's computer it copies every username and password saved in the browser, and those get bundled up and traded. If a member of staff ever saved a work login on an infected machine, their council address and password can end up on a list anyone can buy. We never see or try those passwords, only that records exist against a council's domain and how many. **We cannot tell whether any still works**, only that the material is out there.

122	4	0
councils with staff passwords circulating, 506 records	records on a typical affected council: wide, not deep	ransomware listings, breach records or browser warnings anywhere

The shape matters. Four records on an affected council, 506 across UK local government, is modest for a sector employing over a million people. Broad and shallow: many councils with a handful each, not a few with hundreds. **That makes it finishable.** A reset, a multi-factor check and an ended session deals with most of it.

Why some councils have a floor score rather than an exact one

The change that matters for reading every table in this report

Some council websites answer an automated visitor with a protection page rather than the real homepage. That is usually a security control working, but it means we cannot read the instructions the site sends to a browser, and those form part of the score. For **62 councils** that was the only gap, so we publish a **floor score**: every unread instruction counted as absent, "at least this much", so **the true figure can only be the same or higher**. **26** have no published score, and section 16 gives the reason for each.

Scores	Websites	Average
Exact scores	291	76.3
Floor scores, counted at their floor	62	63.7
All published figures, 353 of 379	**353**	**74.1**

Use 76.3 for the sector's measured position and 74.1 for the most cautious one. Were every unread instruction in place, those 62 councils would average 83.7 rather than 63.7. The truth sits between. The remaining 26 have no published figure at all.

What is going well, and it is worth saying

227 councils, six in ten, instruct other mail systems to refuse email forged in their name, and only 17 have not started. Getting there means listing every system that sends mail in a council's name and testing before enforcing, or genuine letters to residents bounce. Councils have largely done it, with no law requiring it, and **all 379 publish the record identifying their own mail servers.**

Exact-score averages sit within about two points of each other, 75.6 in Wales to 77.7 in Northern Ireland, but **will not carry a league table**: the evidence behind each differs and only Northern Ireland needed no floor scores.

What changed since 9 September

Every website was rescanned on 27 September. Before any comparison was drawn, the script that produces these figures was run against the retained 9 September scans and reproduced that edition exactly, so both columns below come from one method.

Measure	9 September	27 September	Reading
Published scores, exact / floor	350 (293 / 57)	353 (291 / 62)	Coverage, not posture: more sites now withhold their homepage from a scanner, or have a fault that stops it reading them.
No score published	29	26	Now explained website by website, in section 16.
Exact-score average	75.6	76.3	On the 285 websites with an exact score on both dates it rose 0.6: 55 up, 18 down, 212 unchanged.
Cautious average	72.9	74.1	Floors counted at their floor on both dates.
Good / at risk, all published	128 / 8	132 / 4	
Privacy / payment checks	61.8% / 89.6%	63.8% / 91.3%	Partly the next row, which removes failures that were really refusals.
Visitors not forced onto a secure connection	63	27	29 were sites refusing our scanner's insecure request, now recorded as unknown rather than a failure (a scanner change on 17 September); 3 now redirect; 4 are unknown for other reasons.
Invalid website certificate	2	0	Both are incomplete certificate chains, now reported as faults in section 12.
Software weakness read from a version	11 / 261	15 / 565	Websites / observations. All read from version numbers.
Actively-exploited catalogue entries	2	3	One new, in Northern Ireland: the same flaw as the English entry.
Risky service, council level / shared	14 / 3	12 / 4	Two no longer answer, one new one does, and one moved to the shared line because its address now also serves an unrelated organisation.
Risky-port observations	**107**	**62**	**One platform provider's addresses now answer on far fewer ports.**

Two corrections to earlier editions

The unscored websites were misdescribed. Earlier editions said the 29 unscored websites lacked "the certificate or the homepage connection". The retained evidence shows 24 of the 29 lacked the mail transport policy, 22 of them nothing else. That is corrected here, and section 16 now gives the reason for each missing score.

Exposure figures. The 9 September column above is this edition's case-by-case method applied to the old scans. Anyone holding an earlier edition's exposure figures should use these.

Why this matters for a council in particular

A council is the organisation a resident cannot choose not to deal with. Council tax, housing, school places, planning, benefits, bin collections, parking, social care: every one of those leaves personal information with an authority the resident has no realistic option to take elsewhere. That is a different relationship from the one a customer has with a shop, and it changes what a failure means.

It also changes what impersonation means. A message that appears to come from a council carries the weight of an institution with legal powers. A demand for council tax, a notice about a benefits claim or a parking penalty gets acted on quickly, and often by the people least able to absorb the loss.

A way of picturing what we did

> **Somebody walking down your street**
>
> They never go inside any building and never try a door. They walk past and notice what is visible from the pavement: a window left open, a side gate unlatched, a spare key under the mat where everyone knows to look.
>
> None of that means the house has been burgled. It means somebody passing by can see opportunities, and most of them take a minute to put right.

That is exactly this assessment. We looked at each council from the public internet, the way any resident or anyone with worse intentions would see it. When this report says staff passwords are circulating, that is the spare key under the mat: it does not mean anyone has used it, but somebody else knows where it is. When it says a service is reachable that need not be, that is the side gate nobody remembers leaving unlatched. And when a council's website turns our scanner away, that is a locked gate doing its job, which is why those councils get a floor score rather than a mark against them.

> **What we could not see, which is most of it**
>
> Standing in the street tells you nothing about the alarm, the safe or the locks on the internal doors. Many of these councils will have good protections we simply cannot observe: staff training, backups, monitoring, incident plans, internal access controls, everything inside the building.
>
> So nothing in this report is a verdict on any council's security. It is an account of what is showing from outside, which is a useful thing to know precisely because it is what a criminal sees too.

Three cautions that apply to every number in this report

A finding is not a break-in. Nothing here establishes that any council has been compromised, and every serious item needs the council to check it privately before anyone treats it as fact.

A floor score is not a bad score. Sixty-two councils carry one, and each could sit substantially higher. They should never be compared with exact scores or ranked against them.

Nothing here is a compliance judgement. We observe technical settings. We cannot see contracts, retention, staff training or how personal information is actually handled, and this report never pretends otherwise.

1. The words used in this report

This section exists so that nothing later needs a specialist to interpret. Each term is given the way it is used here, not as a formal definition.

Term	What it means in this report
Cyber posture	The condition of an organisation's defences at a point in time, as seen from outside. If a stranger looked at your council from the public internet, what could they learn?
Criminal credential collection	A traded list of usernames and passwords, mostly harvested by viruses from the browsers of infected computers. Also called infostealer data.
Floor score	A score published as "at least this much" where one part of the check could not be read. Every unread item is counted as missing, so the true figure can only be the same or higher.
Forged email, and the setting that stops it	Anyone can put a council's name on an email. A published instruction called a **DMARC policy** tells receiving mail systems to refuse those forgeries. It can be set to refuse, to send to spam, or to do nothing.
Mail transport policy	A published instruction (MTA-STS) telling other mail systems to deliver the council's email only over a protected connection. The policy itself is a file on a web address; if that file cannot be fetched, the protection does not operate.
Secure connection	The padlock. A page served over HTTPS is encrypted in transit; one served over plain HTTP can be read or altered on the way. Forcing every visitor onto the secure version is a setting.
Exposed service	Something answering the public internet that normally faces inwards: a database, a remote-access tool, a file-transfer or admin console.
Known-vulnerability evidence	A public source records a documented weakness against software the website appears to be running. It may already be patched; it needs checking.
Cookie consent mechanism	The banner that asks permission before storing things on a visitor's device. The law governs what may be stored before a choice is made.
Website instructions to the browser	Settings a website sends telling the browser how to treat the page. Their absence is a review point, not a hole. These are the items a floor score counts as missing.
Certificate, and its chain	The credential that proves a website is who it claims to be and enables the padlock. It is vouched for by a chain of issuers; a server that leaves out part of the chain is refused by many systems.

Security is cumulative, which is why there is no single fix

A strong position is rarely one product. It is the combined effect of many ordinary settings done properly: strong sign-in, sensible configuration, secure email, patched software, limited exposure to the internet, knowing what suppliers hold, a clear route for someone to report a problem, and a plan for when something goes wrong.

That is also why a good score can sit alongside a real finding, and why one serious item can hold an otherwise well-run website down a band.

2. Where councils sit in the rules

Councils occupy an unusual position, and it explains a good deal of what this report found.

Security: no legal duty specific to councils

Councils hold some of the most sensitive personal information in the public sector and run services residents cannot get anywhere else. Yet **they are not designated as operators of essential services** under the main UK cyber security regulations, and there is no dedicated regulator for council cyber security the way there is for aviation or energy.

What exists instead is help rather than obligation. The government adapted the National Cyber Security Centre's Cyber Assessment Framework for local government, working with councils, and published it as a tool authorities can use to assess themselves.[2] The Cyber Security and Resilience Bill, currently before Parliament, largely leaves councils outside its scope: it targets essential service operators, digital providers, data centres, managed service providers and designated critical suppliers. The Local Government Association supports the supply chain and incident reporting parts while pressing for clarity, support and realistic timescales, noting legacy systems and limited in-house expertise.[3]

> **A result worth sitting with**
>
> On the one control this assessment measures that most directly protects residents from being defrauded in a council's name, local government performs strongly, and it does so with no law compelling it. That is an argument about what shared support and central guidance achieve, and the evidence makes it rather than us.

Data protection: a duty that does apply, directly

Where the security regime is voluntary, data protection is not. Councils are legally responsible for the personal information they hold about residents under the UK GDPR, and separate rules govern what may be stored on a resident's device when they visit a website. The Information Commissioner's Office regulates both and publishes the guidance that decides whether a particular arrangement is lawful.[4]

> **What this report can and cannot say about that**
>
> We can see whether a website forces a secure connection, whether a privacy policy can be found, whether a cookie banner is present in the page as delivered, and what the website stores. **None of that establishes whether a council is complying with anything.**
>
> We cannot see the lawful basis for any processing, how long information is kept, what contracts are in place with suppliers, whether information leaves the country, how requests from residents are handled, or any of the training and internal controls that make up most of the regime. Those are the substance. We observe the shop window.

How this differs from the statistics you may have seen

Most sector cyber figures come from surveys, which ask organisations what happened to them and what they have in place. This study asked nobody anything. Every number is an observation taken from outside using the same checks on every website. A survey tells you what a sector believes about itself; this tells you what it is showing to the world.

3. What we measured, and how to read the numbers

Each website was checked against the same set of external tests and given a score out of 100 where enough evidence came back. **Good** is 75 or more, **needs improvement** is 50 to 74, and **at risk** is below 50.

Coverage	England	Wales	Scotland	N Ireland	UK
Tracked websites	314	22	32	11	379
Completed a scan	314	22	32	11	379
Exact score	243	18	19	11	291
Floor score	49	4	9	0	62
No score published	22	0	4	0	26
Any published figure	**292**	**22**	**28**	**11**	**353**

Why different numbers here have different denominators

Not every test could answer for every website, so a percentage in this report always states what it is a percentage of. The main groups are:

379 tracked websites, all of which completed a scan, used for stolen-password findings, exposed services and most technical checks. **291 exact scores**, used for the measured average and bands. **353 published figures**, used for the cautious average. And **narrower groups** for individual tests: 308 websites returned a readable page for the browser-instruction and tracking checks, and 301 gave cookie evidence.

Every table shows the count and its denominator together, in the form 201 / 257 readable, with the rate beside it. Where a test returned an unknown for some websites, the denominator is the number that actually answered, because an unknown is not a pass.

Three rules this report follows throughout

Counts are of websites, not of problems. A website with five instances of the same issue counts once. One unpatched piece of software can generate dozens of technical observations, which is why we report the number of councils affected and not the number of observations.

Rows in a table overlap and must never be added. The clearest case: 12 councils have a risky service and 10 have a database port, but the 10 are inside the 12. The total is 12 councils, not 22.

Stolen passwords come in three separate populations, covering different people and fixed by different parties. Section 9 sets them out. They are quoted independently and never combined into one headline number.

4. Source one: England, 314 websites

England is 83% of the estate, so its result largely determines the UK figure. All 314 completed a scan. 243 produced an exact score, 49 a floor score and 22 no score. **All three confirmed lowest-band results in the UK are here.**

Band	On exact scores 243 websites	Including floor scores 292 websites
Good, 75 and above	106 (44%)	107 (37%)
Needs improvement, 50 to 74	134 (55%)	181 (62%)
At risk, below 50	3 (1.2%)	4 (1.4%)

Exact average **76.3**, median **74**. Counting the 49 floor scores at their floor gives **74.2**. Those floors average 63.6 and would average 83.7 if every unread instruction turned out to be in place, so the extra At risk result in the right-hand column may sit higher.

Observation	Websites	Rate
No cookie consent mechanism detected	201 / 257 readable	78%
Tracking technology present	187 / 257 verified	73%
No privacy policy route found	47 / 240 answered	20%
Visitors not forced onto a secure connection	24 / 264 answered	9%
Cannot refuse forged email in the council's name	14 / 314 tracked	4.5%
Fault on the council's own systems	12 / 314 tracked	3.8%
Software with a publicly listed weakness	12 / 314 tracked	3.8%
Outdated encryption still accepted	11 / 295 answered	3.7%
Risky service reachable, at council level	10 / 314 tracked	3.2%
Secure page loading insecure content	8 / 257 readable	3.1%
Database port answering, at council level	8 / 314 tracked	2.5%
Invalid certificate, ransomware, breach, browser safety	**0 / 314 tracked**	**0%**

England carries almost all of the exposure work. Fourteen websites showed a risky service: **ten are council-level cases**, two with a product identified and one of those a database, and four sit on addresses shared with unrelated organisations and are reported separately. All 524 software-weakness observations were read from version numbers, two websites on one hosting platform holding 238 of them, and one carries an actively-exploited catalogue entry on a hosting provider's address.

5. Source two: Wales, 22 websites

Every Welsh website carries a published figure: 18 exact scores and 4 floor scores, with none left unscored. The exact average is **75.6**, median **74.5**, the lowest of the four estates, and no website is in the lowest band on either basis. **No Welsh council has a fault on its own systems** of the kind found in England and Scotland.

> **Wales holds both extremes in this study**
>
> **Not one of the 18 readable Welsh homepages showed a cookie consent mechanism.** That is the only estate with a complete absence, and the strongest single prompt for browser testing in the report.
>
> **Every Welsh council can refuse forged email in its name**, 14 set to refuse and 8 to send to spam, with none doing nothing. Wales is the only estate with no gap at all on that control.

Band	On exact scores 18 websites	Including floor scores 22 websites
Good, 75 and above	9 (50%)	9 (41%)
Needs improvement, 50 to 74	9 (50%)	13 (59%)
At risk, below 50	0	0

Counting the four floors at their floor gives **73.5**. Those floors average 64.5 and would average 76.2 with every unread instruction in place, the narrowest gap of any estate.

Observation	Websites	Rate
No cookie consent mechanism detected	18 / 18 readable	100%
Tracking technology present	8 / 18 verified	44%
No privacy policy route found	6 / 16 answered	38%
Mail signing record missing on the names we sampled	5 / 22 tracked	23%
Address flagged on public reputation sources	3 / 22 tracked	14%
Outdated encryption still accepted	2 / 21 answered	10%
Visitors not forced onto a secure connection	1 / 19 answered	5%
Risky service, database, listed software weakness	1 each / 22	5%
Forged email, own-system fault, invalid certificate, insecure content, ransomware, breach, browser safety	**0 / 22 tracked**	**0%**

Wales's risky service, exposed database and software weakness are **the same single website**, on a hosting address with no sign of unrelated organisations on it, where a file-transfer and a database service were both identified by name. It is a credible council-level finding, not a provider artefact. Its 35 software observations were all read from version numbers and **none appears in the actively-exploited catalogue**. A flagged address can belong to another tenant, so ownership comes first.

6. Source three: Scotland, 32 websites

Scotland's exact average is **76.2**, median **76**, on 19 websites. Nine carry a floor score and four have none, so the exact average describes only three websites in five.

Band	On exact scores 19 websites	Including floor scores 28 websites
Good, 75 and above	10 (53%)	10 (36%)
Needs improvement, 50 to 74	9 (47%)	18 (64%)
At risk, below 50	0	0

Counting the nine floors at their floor gives **72.3**. **Scotland has the widest floor-to-ceiling gap of any estate**, 64.1 against 87.4, so those nine websites are the least well understood in the study. Two of them are floors because of a fault or a server error on the council's side, not a protection page.

Observation	Websites	Rate
No cookie consent mechanism detected	19 / 22 readable	86%
Tracking technology present, all one product	13 / 22 verified	59%
No privacy policy route found	8 / 18 answered	44%
Mail signing record missing on the names we sampled	6 / 32 tracked	19%
Fault on the council's own systems	**4 / 32 tracked**	**13%**
Visitors not forced onto a secure connection	2 / 25 answered	8%
Outdated encryption still accepted	2 / 31 answered	6%
Secure page loading insecure content	1 / 22 readable	5%
Software weakness in the actively-exploited catalogue	**1 / 32 tracked**	**3%**
Cannot refuse forged email in the council's name	1 / 32 tracked	3%
Risky service, database exposed, invalid certificate, ransomware, breach, browser safety	**0 / 32 tracked**	**0%**

The single most specific finding in the whole study is in Scotland

Scotland's risky-service case from 9 September no longer answers. The software weakness is a different website, and a different order of concern. **It runs web server software with two recorded weaknesses. One appears in the public catalogue of weaknesses criminals are known to be exploiting now**, a far shorter and more serious list than "recorded somewhere", and the product is marked past the end of its supported life, so no more fixes are coming. What makes it stand out is the address: most exposure evidence points back at a hosting company, but **this one is registered to the local authority itself**. Both observations were read from a version number rather than confirmed, so check the running version first, quietly and directly with the council. **If one thing in this report is acted on this week, it is this.**

Council identities on other companies' platforms reach 78% of Scottish websites, against 56% in England and the widest footprint in the study. Credential figures for all four estates are compared in section 9.

7. Source four: Northern Ireland, 11 websites

Northern Ireland is the only estate where every website produced an exact score. No floor scores were needed anywhere, which means it is also the only estate whose figures are fully comparable within themselves. The average is **77.7**, median **76**, the highest of the four.

> **Complete evidence is not the same as a good result**
>
> Full coverage means the information was collectable, not that the estate is in good order. Northern Ireland has the highest rate of outdated encryption of any estate, 4 of 11, the highest rate of councils unable to refuse forged email, 2 of 11, the lowest payment-surface score of the four, and since 9 September its first actively-exploited catalogue entry. Those things are easy to confuse and this is the clearest illustration of the difference in the study.

Band	Websites	Share of 11
Good, 75 and above	6	55%
Needs improvement, 50 to 74	5	45%
At risk, below 50	0	0%

Observation	Websites	Rate
Tracking technology present	10 / 11 verified	91%
No security contact file (security.txt) published	7 / 9 answered	78%
No cookie consent mechanism detected	5 / 11 readable	45%
Outdated encryption still accepted	**4 / 10 answered**	**40%**
No privacy policy route found	2 / 10 answered	20%
Cannot refuse forged email in the council's name	2 / 11 tracked	18%
Software weakness in the actively-exploited catalogue	**1 / 11 tracked**	**9%**
Risky service and exposed database on one website, insecure content on another	1 each / 11	9%
Own-system fault, invalid certificate, insecure connection, ransomware, breach, browser safety	**0 / 11 tracked**	**0%**

Its single exposed service is genuine: a hosting address with no sign of unrelated organisations, where a file-transfer and a database service were identified by name, one of only three identified council databases in the UK. The new weakness evidence is four observations on one website, all read from version numbers; one is a browser-side flaw in an old version of a widely used scripting library, on a cloud provider's address, and updating the library removes it. **Northern Ireland also has the lowest credential exposure in the study on all three populations.** On an estate of eleven a single council moves any percentage by nine points.

8. The four estates compared, and the UK total

All four were rescanned the same day with the same checks. **This is not a league table**: the estates do not carry equal evidence.

Measure	England	Wales	Scotland	N Ireland	UK
Websites, all completed	314	22	32	11	379
Exact / floor / no score	243/49/22	18/4/0	19/9/4	11/0/0	291/62/26
Exact average / median	76.3 / 74	75.6 / 74.5	76.2 / 76	77.7 / 76	76.3
Cautious average, floors at floor	74.2	73.5	72.3	77.7	74.1
Confirmed lowest band	3	0	0	0	3
Fault on the council's own systems	12	0	4	0	16
Risky service, all cases	14	1	0	1	16
of which council-level database ports 10, of which 3 identified	**10**	**1**	**0**	**1**	**12**
on a shared address, reported separately	4	0	0	0	4
Software weakness read from a version	12	1	1	1	15
Weakness in the actively-exploited catalogue	**1**	**0**	**1**	**1**	**3**
Staff passwords in criminal lists	33%	36%	28%	18%	32%
Identities on other platforms	56%	59%	78%	36%	57%
Cannot refuse forged email	4.5%	0%	3%	18%	4.5%
Outdated encryption accepted	3.5%	9%	6%	36%	5.0%
No consent mechanism detected	78%	100%	86%	45%	79%

Rates are of tracked websites, except consent, of readable homepages. In Wales and Northern Ireland one council moves a rate by several points.

What is national, and what is local

Four findings hold everywhere. Forged email is refused or filed to spam almost universally. Exposed services are rare, 12 council-level cases in 379. Consent mechanisms are weakly detected everywhere. And every estate returned nothing on ransomware, breach records and browser safety warnings.

Four findings are local and should not be generalised. Outdated encryption is 3.5% in England against 36% in Northern Ireland; identities on other platforms 78% in Scotland against 36% in Northern Ireland; all three confirmed lowest-band results are English; and faults on councils' own systems were found only in England and Scotland.

The UK total

No website appears in two estates, so the four add to **379 distinct websites**. Exact scores average **76.3** across 291 (131 Good, 157 needing improvement, 3 at risk); with floors at their floor, **74.1** across 353 (132, 217, 4). **The extra at-risk result is a floor and may sit higher.**

9. Stolen credentials: three different problems

This is the largest and most misunderstood body of evidence in the report. The provider returns three separate populations, they concern different people, they are fixed by different parties, and **they must never be added into one number**. Counts were returned and reconciled for all 379 websites.

Population	Who it concerns, and who can act	Websites	Rate	Records
1. Staff	Accounts on the council's own domain. **The council can fix these today** by resetting the password, ending active sessions and confirming multi-factor sign-in.	122 / 379	32.2%	506
2. Identities elsewhere	Council email addresses used to sign in to other companies' platforms. The council can act, but the reset happens on the other company's system.	217 / 379	57.3%	949
3. Residents	Members of the public with an account on a council service, whose own device was infected. **Nobody at the council can reset these.** Only the resident can.	359 / 379	94.7%	46,948
1 or 2	**Deduplicated. Not 122 plus 217.**	**230 / 379**	**60.7%**	**n/a**

Why the order matters more than the size

The staff population is the one that matters and it is the smallest. It is a key to the council's own systems, the council issued it, and the council can take it back this afternoon.

The identities-elsewhere population follows closely, because a work address reused across several platforms is how one compromise becomes several.

The residents population is ninety times larger and ranks last. It is not access to anything the council runs. It is a resident's own laptop that caught a virus. It carries no weight in the score and nobody at the council can reset it. It is a duty-of-care and communication question, not a security hole.

Reported as one total of 48,403 this would describe a sector in serious trouble. Reported as three populations it describes a manageable job, a wider hygiene question, and a public-protection issue belonging to a different team.

What 'identities elsewhere' does not mean

It counts **the council's own email addresses appearing on somebody else's platform**. It is **not** a count of suppliers holding access into the council, which is close to the opposite. Described that way it would claim something this study has not measured, so we never call it a supplier figure.

9 continued: the four estates side by side

Websites carrying records	England of 314	Wales of 22	Scotland of 32	N Ireland of 11	UK of 379
1. Staff	103 (33%)	8 (36%)	9 (28%)	2 (18%)	122 (32%)
2. Identities elsewhere	175 (56%)	13 (59%)	25 (78%)	4 (36%)	217 (57%)
3. Residents	304 (97%)	19 (86%)	29 (91%)	7 (64%)	359 (95%)
1 or 2, deduplicated	**185 (59%)**	**14 (64%)**	**26 (81%)**	**5 (45%)**	**230 (61%)**

Records, and how many per affected website	England	Wales	Scotland	N Ireland	UK
1. Staff	442	14	47	3	506
per affected website	4.3	1.8	5.2	1.5	4.1
2. Identities elsewhere	807	28	107	7	949
per affected website	4.6	2.2	4.3	1.8	4.4
3. Residents	43,129	2,041	1,727	51	46,948
per affected website	**142**	**107**	**60**	**7.3**	**131**

Three things only the aggregated view shows

The two populations that matter are wide and shallow. Both sit at roughly four records per affected council across the UK. Many councils with a handful each, not a few councils with hundreds. That is the shape that makes this finishable.

Scotland is the outlier on reach and England on volume. Scotland has the widest footprint, 81% of its websites carrying something the council can act on. England holds 86% of the actionable records, a little ahead of its 83% share of the estate.

The residents population behaves like a different measurement entirely, from 7.3 records per affected website in Northern Ireland to 142 in England. That twentyfold spread tracks population served and how many residents hold online accounts, not security. It is the clearest reason never to fold it in with the other two.

What these records establish, and what they do not

They are public-source records tied to a council's domain, mostly harvested by viruses on individual computers. **We cannot see whether any password still works, whether the account still exists, or when the infection happened.** The source does not tell us how completely it has collected, so we make no claim that this is fresh or complete.

None of it is evidence that a council has been broken into. It is a reason for each council to check its own accounts privately against its own records, and never by trying a recovered password.

10. Cookies, consent and tracking

This is the largest body of evidence in the report and the one that concerns what happens on a resident's own device. It also sits in the regime that applies to councils directly.

> **Read this before the number**
>
> Our privacy check scored **63.8% of the points it was able to assess**. **That is not 64% compliant with anything.** It scores a handful of visible technical settings and nothing about how a council actually handles personal information.

What we looked for	Yes	No	Could not tell	Why it matters
Visitors forced onto a secure connection	292	27	60	Anything typed into an insecure page can be read on the way.
No insecure content on a secure page	298	10	71	A padlock is weakened if parts of the page arrive unprotected.
Privacy policy route found	221	63	95	People should be able to find out what happens to their data.
Cookie consent mechanism found	**65**	**243**	**71**	The law governs what may be stored before a person chooses.
Security file links a disclosure policy	41	240	98	The stricter check: of 53 councils publishing a security contact file (section 14), 41 link a policy.

243 of the 308 websites we could read showed no consent mechanism, 79%. The national picture varies more here than on any other measure: 56 detections in England, six in Northern Ireland, three in Scotland and none at all in Wales.

> **An absent banner is a reason to look, not a finding**
>
> There are innocent explanations. The site may store only what is strictly necessary, for which no permission is needed. It may use a system our check does not recognise. It may load the banner later than a single page request sees. **And a banner being present proves just as little**: it does not show that refusing is as easy as accepting, or that nothing was stored before the visitor chose.
>
> The only way to settle any of it is to open the site in a browser and watch. That takes about ten minutes per site and needs no specialist.

10 continued: the regulator is testing this

In December 2025 the Information Commissioner's Office reported the result of testing the **top 1,000 websites used in the UK**. It checked three things: whether advertising cookies were stored before consent, whether refusing was as easy as accepting, and whether cookies were placed without permission at all.

564	17	21
of the 1,000 only became compliant after the ICO contacted them	received preliminary enforcement notices	were still non-compliant when the ICO reported

The ICO said it will keep testing the top 1,000 periodically.[5] Two things follow for councils. An absent consent mechanism is not unusual, since more than half of the UK's most-visited websites needed prompting. And more importantly, **the regulator tests precisely the behaviours this scan cannot see**, so our signal is a prompt to look rather than an answer.

> **What a browser check should establish, in order**
>
> **1.** What is stored on the device before any choice is made, and is any of it not strictly necessary. **2.** Is there a refuse option, is it on the first screen, and does it take no more effort than accepting. **3.** Does refusing actually stop the storage, or just record a preference. **4.** Does the same hold on service pages and forms, not just the homepage. **5.** What does each piece of tracking code load, and what leaves the browser when it does.

Tracking technology, and one vendor's dominance

Tracking technology was present on **218 of the 308 websites we could check, 71%**. One product accounts for almost all of it: Google Tag Manager appears on 211 of those 218, so a single company's code sits on more than two thirds of the readable council web estate. Microsoft Clarity appears on 29, Google Analytics and Facebook Pixel on 2 each and Hotjar on 1, and these overlap.

The presence of tracking code proves nothing on its own. It does not show that personal data was sent, that permission was needed, that permission was missing, or what legal role the vendor plays. A tag manager is a container: what it loads and when has to be watched, not assumed. Microsoft Clarity is worth separate attention because it records sessions rather than counting pages, which raises sharper questions about what is captured and whether form fields are masked.

What the websites store

Cookie evidence came back for 301 websites. **127 stored something during the first page visit, 275 items in total.** Of those 127, 63 stored at least one item without the setting that limits it being sent from other websites, 41 without the setting that keeps it off insecure connections, and 21 without the setting that hides it from page scripts.

This only sees what the first page request returns, so the real numbers are higher. Not every item needs every setting, so this is a review list rather than a defect list: each one needs its purpose, lifetime and necessity looked at together, and that same review answers the consent question above.

11. Card payments and the concrete technical work

Councils take card payments at scale: council tax, business rates, parking, licensing, garden waste, leisure, school meals, rents. The card industry's security standard applies wherever an organisation handles card data or runs something connected to a system that does. Most councils will have arranged their payment pages to send the payer to a specialist provider, which keeps as much as possible out of scope.

> **Two things this report is not**
>
> Our payment-surface check scored **91.3% of the points it could assess**. Controls we could not verify were removed from the calculation rather than counted as passes, which is exactly why that number is high. **It does not mean 91.3% compliant.** Three controls could not be answered for a single council in the estate.
>
> And **this is not the scan the card standard requires.** That standard requires quarterly scans by a company specifically approved by the card industry. We are not one, and nothing here can be submitted as evidence of compliance.[6]

One point makes this newly relevant. Under the current version of the standard, quarterly approved scanning now applies even to the lightest category, the one most councils will be in, following a change that became mandatory in March 2025. The reasoning was that sending a payer off to a provider still leaves the council's own page exposed to code injected before the payer ever gets there.[6] **That is the same page carrying the tracking code in section 10.**

Where the concrete work actually is

3	12	27
run software with a weakness known to be actively exploited	council-level risky services, 10 on a database port	councils do not force visitors onto a secure connection

Twenty-seven councils do not force visitors onto the secure connection, the one item here a resident could notice. A page reached without the padlock can be read and altered on the way, and so can anything typed into it. Separately, 60 of the 308 measured responses do not tell the browser to stop trying the insecure version at all, which leaves the first request of every visit exposed even where a redirect exists. The two belong in one piece of work, and 19 councils still accepting outdated encryption belong beside them.

11 continued: who is actually answering

What is answering on the flagged port	England	Wales	Scotland	N Ireland	UK	Databases
A service identified by name on the flagged port the only cases confirmed to be running something	2	1	0	1	4	3
A content-delivery address used only by that council nothing identified answering	2	0	0	0	2	2
A platform address used only by councils nothing identified answering	5	0	0	0	5	4
Other hosting, nothing identified, no sign of sharing	1	0	0	0	1	1
Council-level cases	**10**	**1**	**0**	**1**	**12**	**10**
An address shared with unrelated organisations nothing identified answering; reported separately	4	0	0	0	4	2
All risky-service cases observed	**14**	**1**	**0**	**1**	**16**	**12**

Rows are exclusive and sum to the totals. Two questions decide each case, from evidence we already held: did a named product answer on the flagged port, and do unrelated organisations use the same address? Of 62 port observations, 44 belong to the 12 council-level cases and 18 to the 4 shared ones.

Who owns the address decides whose list it is on

An address used only by a council, or by partner councils in a shared-service arrangement, is part of its internet presence whoever operates the machine, so those cases stay on the council's list even where the answering equipment is a provider's. Where a provider operates it, the question of what is meant to be reachable goes to that provider.

Four sit on an address genuinely shared with unrelated organisations, all in England, one of them moved there since 9 September because its address now also serves an unrelated organisation. Reported separately because no council can close it alone; a weakness there reaches every organisation on the platform.

What has not changed is how much is confirmed. Only the first row, four websites with three identified databases, has a service we saw running. On the other eight a port answers with nothing behind it that we could identify, which is a question to resolve rather than a fault to report.

The fifteen software-weakness cases produced 565 technical observations between them, 524 on twelve English websites, 35 on one in Wales, two on one in Scotland and four on one in Northern Ireland. **Report the fifteen, not the 565**, and treat even the fifteen carefully: every observation was read from a version number and **not one was confirmed by the provider running it**. Two websites on one hosting platform hold 238 of them, and suppliers routinely apply fixes without changing the version number, so version-read matches overstate the position. Three entries, on three websites, appear in the catalogue of weaknesses known to be actively exploited: two are the same flaw in an old scripting library on provider addresses, in England and Northern Ireland, and the third is the Scottish web server in section 6. **Those three are the ones that matter.**

12. Faults any visitor or mail system would meet

New in this edition. These are not findings about what a council has chosen to show. They are things that are broken, confirmed on 27 September by ordinary requests to the public addresses concerned, the same requests any browser or mail system makes. **Sixteen councils have at least one**, twelve in England and four in Scotland, counted once each. None is named here.

> **A locked gate is not on this list**
>
> A website that turns an automated visitor away is making a legitimate choice, and it is not counted here. Everything below affects ordinary visitors or mail systems too.

Fault	England	Scotland	UK	Fix
Email protection advertised, but its policy file cannot be fetched by anyone the mail transport policy described in section 1	**11**	**3**	**14**	Serve the policy file, or withdraw the published record until it can be served.
of which the policy server's certificate has expired	3	1	4	Renew the certificate.
certificate issued for another name, a hosting platform's	1	1	2	Install a certificate for the policy server's own name.
policy server offers no certificate at all	2	0	2	Switch on the secure connection there.
policy server's certificate chain is incomplete	1	1	2	Send the missing intermediate certificate.
policy server returns an error (not found, forbidden)	3	0	3	Publish the file at the correct path.
policy server's name does not exist	1	0	1	Create it, or withdraw the record.
Website certificate chain incomplete	**2**	**0**	**2**	Send the intermediate certificate with the site's own.
Address typed without "www." sends every visitor to a malformed address	**0**	**1**	**1**	**Correct the redirect rule.**

One English council has both an incomplete website chain and a failing policy server, which is why the bold rows sum to 17 rather than 16.

Why each one matters. A mail transport policy that cannot be fetched protects nothing: sending mail systems cannot read it, so the protection the council has advertised does not operate, and the website carries no score. A browser often repairs an incomplete certificate chain on its own, but many other systems, older devices and automated services reject the connection. And anyone who types the council's address without "www." reaches an error page.

Advertising a mail transport policy is a good step, and these councils have taken it. The fault is only that the file is not being served. Every item here is a configuration change with a clear fix.[1]

13. Forged email: the sector's best result

Anyone can put a council's name on an email. What stops it reaching the inbox is a published instruction telling receiving mail systems what to do with a message that fails the checks. It can say refuse, send to spam, or do nothing.

What the council publishes	England	Wales	Scotland	N Ireland	UK	Share
Refuse the forgery	193	14	15	5	227	60%
Send it to spam	107	8	16	4	135	36%
Do nothing, monitoring only	12	0	1	2	15	4%
Nothing published, or unclear	**2**	**0**	**0**	**0**	**2**	**0.5%**

Two figures, both true, and they answer different questions. Only 17 councils, 4.5%, publish nothing or monitoring-only, and those are the ones with work to start. But 135 more ask only for spam filing rather than refusal, so 152 do not ask for outright refusal. **The 4.5% identifies who needs to begin; the 60% describes how far the sector has actually got.**

The work behind this is harder than the result suggests. Publishing the instruction takes minutes. Doing it safely does not: a council has to know every system that sends mail in its name, the customer system, the payments provider, the schools mailer, the parking contractor, the consultation platform, the recruitment system, and watch for long enough to be confident, or genuine letters to residents start being refused.

> **Spam filing is a staging post, not a destination**
>
> The right sequence is watch, then file to spam, then refuse. A council already filing to spam has done most of the work and should finish. A council doing nothing should not jump straight to refusal: list the legitimate senders first, or it will stop its own benefits notifications reaching the people who need them.

This describes what a council asks other mail systems to do. It does not prove a forgery would in fact be refused, because receiving systems apply their own judgement, and it does not prove every genuine sender is set up correctly. Supporting records are strong: all 379 councils publish the basic record identifying their mail servers, and 348 had a signing record under the names we sampled, with 31 not found. A name we did not sample may still exist.

14. Two settings almost nobody has, and one dependency nobody records

Setting	Have it	Do not	What it does
Mail server record	379	0	Names which servers may send mail for the council. Universal.
Mail signing record	348	31	Signs outgoing mail so it can be verified. Sampled, so absence is not conclusive.
Encryption reporting	235	144	Asks other systems to report failures in protecting mail in transit.
Security contact file (security.txt) published	53	230	Tells a researcher where to report a problem privately. 41 of the 53 also link a disclosure policy.
Certificate authority record	42	337	Names which companies may issue certificates for the domain, so a rogue one is refused.
Signed domain records	**8**	**371**	**Stops someone forging the answer to 'where is this council's website'.**

Eight councils out of 379 have signed domain records, 2%. Seven in England and one in Northern Ireland, none at all in Wales or Scotland. The certificate authority record sits at 11%. **A gap shared by nine councils in ten is a sector fact, not 371 individual failures**, and it is a natural candidate for central guidance rather than 379 separate projects.

The security contact file deserves its own note. 53 councils publish one and 230 do not, with 96 we could not determine. Someone who finds a problem at one of those 230 has no obvious way to tell them privately, which is how problems end up made public instead.[1]

The dependency that is on nobody's risk register

Observation	England	Wales	Scotland	N Ireland	UK
Some form of network concentration	256	21	27	9	313
All address records with one provider	246	9	21	10	286
Mail transport policy finding	184	15	16	8	223
Address flagged on public reputation sources	**5**	**3**	**2**	**0**	**10**

These overlap and must not be added. A flagged address can belong to another organisation sharing the same infrastructure, so ownership needs confirming first.

286 councils, three in four, depend entirely on one company to answer the question 'where is this council's website'. That is not a fault. Concentration is usually the better-resourced and better-run choice, and splitting the job across providers brings its own problems. **The question is whether anyone has written it down.** A council that has consciously accepted a single provider and knows what happens if it fails is in a different position from one that has never considered it, and on this evidence the arrangement is close to universal and unlikely to appear on many risk registers.

Domain expiry and transfer-lock observations are deliberately excluded from this report. The public evidence does not show whether automatic renewal is switched on and is not reliable enough to support a finding either way.

15. Old hostnames, seen through certificate records

Every public certificate names the websites it covers. Reading those records for a council turns up hostnames it has used over the years, many of which nobody now remembers running. We reviewed them for all 379 councils, after the 27 September scans.

Observation	England	Wales	Scotland	N Ireland	UK
Councils reviewed	314	22	32	11	379
Related hostnames found	24,207	1,648	3,242	218	29,315
Councils with more than 50 hostnames	156	15	27	0	198
Hostnames reviewed one by one	11,981	961	1,452	218	14,612
Hostnames beyond the review limit	12,226	687	1,790	0	14,703
Reviewed hostnames that could not be assessed	131	8	5	1	145
Councils with hostnames seen only in expired certificates	312	21	32	10	375
Hostnames seen only in expired certificates	**13,681**	**915**	**1,923**	**132**	**16,651**

The rows overlap and must not be added together. The review is bounded: up to 50 related hostnames are reviewed for each council, so a council with more has some it was not possible to read.

57% of the hostnames found, 16,651 of 29,315, appear only in expired certificates. They once had a certificate and may since have been abandoned. That is the point of looking: an old name that still points at a service nobody maintains is the kind of loose end that gets overlooked, because nobody remembers it exists. Most of these will be harmless, and the list is a clean-up job, not a finding.

Four English councils carry 11 loose ends among the hostnames reviewed. In 2 cases a published address points at a target that does not exist. In 9 a hostname's response resembles a hosting service that has not been set up. None was found in Wales, Scotland or Northern Ireland. Each is worth checking, but none is evidence that anyone else controls it: the review did not test who controls any resource.

> **What this does not show**
>
> The review ran for all 379 councils, but its coverage is complete for 150 and partial for 229, and it reads only a bounded sample where a council has more than 50 hostnames. Hostnames that never had a certificate, or that sit behind a wildcard certificate, may be missing. **No finding here is proof that a council has no old hostname**, and none is proof that it has been compromised. The reviews carry their own dates and change no score.

16. The 88 websites we could not fully read

Sixty-two councils carry a floor score and 26 have no score at all. Together that is 88 websites, 23% of the estate. **For this edition every one of the 26 was checked individually, including from outside our scanner**, and the reasons are not all the same.

Why no score was published	England	Scotland	UK
A fault on the council's own systems 14 unreadable mail transport policies and 1 incomplete certificate chain, in section 12	12	3	**15**
The mail transport policy server did not answer our scanner readable from the UK but not from either of our scanning networks	5	0	**5**
The website did not answer our scanner at all probably blocking it; it may work for visitors	5	1	**6**
No score published	**22**	**4**	**26**

Wales and Northern Ireland have none. The five in the middle row publish a policy anyone in the UK can read but our scanning networks cannot, so they probably filter cloud-hosting addresses. We do not work around that: the evidence stays unknown. Six more were in the same position until fixes to our scanner that day let their checks complete.

> ### The 62 floor scores: mostly a locked gate, not a hole in the fence
>
> A floor is published where the only thing we could not read was the set of instructions a website sends to a browser, usually because the site answered an automated visitor with a protection page. That is a security control working, and **it cannot be fixed from our side** without the council or its provider choosing to let a known scanner through. A few floors are not a protection page but a fault or a server error on the council's side, such as the malformed redirect in section 12.

Every one of the 88 was scanned and produced findings, and those findings are counted in every table in this report. Do not put off a real finding because its website has a floor score or none. That is the single most important handling instruction in this document.

What else we could not see

Evidence type, of 379 scanned	Got it	Partly	Could not
Encryption and certificates	371	0	8
Domain registration details	370	0	9
Website instructions to the browser	308	0	71
What the website stores on a device	301	0	78
Other systems on the same infrastructure	28	203	148
Direct mail server test	41	0	338
Cloud storage discovery	**0**	**379**	**0**

These limits apply to scored websites too. The infrastructure source was largely unavailable during this rescan, a limit on our collection, not a change at the councils. Cloud storage appears as unknown, never as a pass.

17. What to do, in order

Ordered by consequence, not ease. These groups overlap and are not a count of separate councils.

1

Deal with the three actively-exploited weaknesses this week

Start with the Scottish case: an address registered to the council itself, web server software past the end of its supported life, and an entry in the catalogue of weaknesses criminals are using now. The other two are the same old scripting library on provider addresses, in England and Northern Ireland; updating the library removes them. Confirm the running version first, and go to the council privately.

2

Check the 12 council-level exposed services, the 4 identified ones first

Ten sit on a database port. Only four have a service we actually saw running, three of them databases, one each in England, Wales and Northern Ireland: start there. On the other eight a port answers and nothing identifiable sits behind it, so the first question is whether anything is listening at all. Where a provider operates the address, the question goes to the provider, but the case stays on the council's list.

3

Ask the providers about the 4 shared addresses

Four English cases sit on addresses that also serve unrelated organisations. No council can close those alone, which is why they are reported separately, but a weakness there reaches every organisation on the platform.

4

Fix the 16 confirmed faults

Fourteen unreadable mail transport policies, two incomplete certificate chains and one malformed redirect. Each is a configuration change with a clear fix, set out in section 12. For fifteen of these councils the fault is also what is withholding a published score.

5

Check the three confirmed lowest-band results privately

All three are in England. Confirm each is real and belongs to the council before it is treated as fact. The fourth at-risk result is a floor score: resolve it by reading the missing evidence, not by treating it as a finding.

6

Reset the staff passwords

122 councils, 506 records, roughly four each. Reset, end sessions, confirm multi-factor sign-in, never test a recovered password. Then the 217 councils with identities on other platforms, where the reset happens elsewhere.

7

Force every visitor onto a secure connection

27 councils. Pair it with the instruction that stops the browser trying the insecure version first, missing on 60 measured responses, and retire the outdated encryption still accepted by 19. Test for compatibility before switching anything on.

17 continued: what to do, in order

8

Open the 243 websites in a browser and watch what happens

The largest group in the report and the one that cannot be settled from outside. Ten minutes per site, Wales first, where nothing was detected anywhere.

9

Finish the email work, carefully

17 councils publish nothing or monitoring-only: list every legitimate sender, watch, then enforce, never jumping straight to refusal. The 135 filing to spam have done most of it and should complete.

10

Publish a security contact file, and look at the near-universal gaps

230 councils publish no security contact file (security.txt), and 12 of the 53 that do link no disclosure policy we could find. Signed domain records sit at 2% and certificate authority records at 11% sector-wide, making both a job for central guidance rather than 379 separate projects.

11

Write down the provider dependency, and handle residents' records proportionately

286 councils rely on one company for their address records: know the failure route and who owns it, rather than change it. 46,948 resident records need proportionate protection, and no council should be called breached because of them.

12

Decide whether to let a known scanner through

The 62 floor scores, the 6 websites that did not answer and the 5 mail policy servers that turn our networks away are cases where the site's edge does not serve a scanner. That is a legitimate control. The choice is whether a complete external picture is worth letting a known scanner through; until then those controls stay unverified.

13

Remove old hostnames that point at nothing

Four English councils carry 11 loose ends: 2 published addresses that point at a target that does not exist, and 9 hostnames whose response resembles a hosting service that was never set up. Check each privately; none is evidence that anyone else controls it. Beyond those, the 16,651 hostnames seen only in expired certificates are a clean-up list, not a finding.

Conclusion

Councils are strong where an attacker would come at them directly, and weak where a regulator would look. Six in ten refuse forged email outright and only 17 have not started. Exposed services remain rare: 12 council-level cases in 379, of which only three are a database we actually saw running. There is not one ransomware listing, breach record or browser safety warning anywhere in 379 scans. None of that is required by law, because councils sit outside the main cyber regulations and largely outside the Bill going through Parliament.

The privacy picture runs the other way. **243 websites showed no consent mechanism and tracking code was found on 218**, in the one regime that does apply to councils directly and has a regulator actively testing it. The security rules councils are outside are the ones they are handling well; the data protection rules they are firmly inside hold the largest body of unresolved evidence.

> ### Where the work actually is
>
> **165 councils, 44%, carry at least one of the genuinely serious items**, 55 once staff passwords are set aside. Three actively-exploited software weaknesses, 12 council-level exposed services, 16 councils with a fault on their own systems, three confirmed lowest-band results, 27 without a forced secure connection and 122 with staff passwords circulating. That is a finishable list, not a sector in crisis, and the sharpest items number three.
>
> **243 need ten minutes in a browser.** Cheap to investigate, and the regulator is already testing it elsewhere.
>
> **Most of the 88 websites we could not fully read need a decision rather than a fix.** Their protection turns our scanner away, which is a control working. The exception is the fifteen whose missing score comes from a fault of their own, which a configuration change will close.

Three things this report does not claim. It does not say any council has been broken into: we could not see inside one and did not try. It does not rank the four nations, because the amount of evidence behind each average differs and one estate needed no floor scores at all. And it makes no compliance judgement of any kind, because we observe settings, not lawfulness.

One thing it does claim. Where a finding is concrete, a floor score or a missing score is not a reason to wait. Three actively-exploited weaknesses, 12 council-level exposed services, 16 faults, 230 credential cases, 27 insecure connections and 243 consent cases can be worked today, and every one should be checked privately before it is acted on or disclosed.

About this report

Produced with MyDomainRisk, a tool developed by Huro Data Technologies Ltd, which has a commercial interest in this analysis and declares it here so readers can weigh it. Every observation was made from outside using public websites, domain records, certificates, cookies and public threat intelligence. Nothing was logged into, no password was tried and nothing was exploited. It is not certification, an audit, legal advice or regulatory advice.

How to read the figures

Bands, and what a score is

Good is 75 and above, **needs improvement** is 50 to 74, **at risk** is below 50. One serious finding can hold a website below a band however much else is right. **A score is a floor, not a verdict**: it records what was visible from outside on one day, not internal controls, patching, training, incident readiness or legal compliance.

Exact scores and floor scores

291 websites have an exact score and 62 a floor score, published as "at least this much" where the browser instructions could not be read. **Floor scores count every unread item as missing**, so the true figure can only be the same or higher, and the bands they fall into may be understated. They are never compared with exact scores or used to rank a council. Two averages are given throughout: **76.3** on exact scores alone and **74.1** counting floors at their floor.

Which population each number comes from

Credential findings, faults and exposed services are shares of **379 tracked websites**; bands and averages are shares of the **291 exact** or **353 published** figures as stated. Individual checks use narrower groups, stated in each table. Where a check returned an unknown, the denominator is the number that answered.

Counting

Every figure counts **websites, not problems**. One unpatched service can produce dozens of observations, which is why councils are counted. Rows overlap and must never be added: the 10 council-level database ports sit inside the 12 council-level services, and the 3 actively-exploited weaknesses inside the 15 read from version numbers.

Exposure is reported by owner, decided case by case. A case counts against the council where a service was identified on the flagged port, or where the address serves only that council or its shared-service partners, whoever operates the machine. It is separated only where nothing was identified and unrelated organisations share the address. Of 16 observed, **12 are council-level and 4 shared.**

The two percentage scores are not compliance rates

The privacy check scored 63.8% and the payment-surface check 91.3% **of the points each was able to assess**. Controls that could not be verified from outside were removed from the calculation rather than counted as passes, which is why the payment figure is high. Neither may be described as a percentage of compliance with anything.

> **Publication rule**
>
> Do not describe an individual council as 'at risk', as non-compliant, or as having a consent failure on this evidence alone. Everything serious needs the council to check it privately first. A website that refuses an automated scanner is exercising a security control, not showing a weakness. And do not attribute a provider's infrastructure to a council.

Notes

Every figure describes the 27 September 2026 rescan. The only comparison is the change table, whose 9 September figures were reproduced exactly from retained scans. Resident records are unscored. The population is tracked websites, not legal authorities; a zero means a check ran and found nothing.

Sources and notes

[1] National Cyber Security Centre

10 Steps to Cyber Security; Email security and anti-spoofing, including the staged move from monitoring, through spam filing, to refusal, and mail transport security; Vulnerability disclosure toolkit; Using TLS to protect data; Multi-factor authentication for corporate online services. Free plain-English guidance requiring no specialist team. ncsc.gov.uk

[2] Cyber Assessment Framework for local government, Ministry of Housing, Communities and Local Government

The NCSC framework adapted for councils by MHCLG working with local authorities, structured around managing risk, protecting against attack, detecting events and minimising impact. Published as a self-assessment tool, not a statutory duty. Page last updated 15 January 2026. security.gov.uk and localdigital.gov.uk

[3] Local Government Association, Cyber Security and Resilience Bill: policy briefing

Councils are largely outside the Bill's direct scope, which targets operators of essential services, digital providers, data centres, managed service providers and designated critical suppliers. The LGA welcomes the supply chain, incident reporting and threat intelligence provisions while pressing for clarity, support, realistic timelines and a unified approach to supplier assurance. Future regulations could introduce duties for councils themselves. At committee stage. local.gov.uk

[4] Information Commissioner's Office

Guide to PECR: cookies and similar technologies, governing what may be stored on a person's device and the permission needed, and A guide to data security under the UK GDPR. These decide whether an arrangement is lawful; the signals in sections 10 and 11 of this report are technical observations and are not such an assessment. ICO cookie guidance and ICO data security guidance

[5] Information Commissioner's Office, ICO action secures increased cookie compliance, December 2025

The ICO tested the top 1,000 websites used in the UK against three requirements: no non-essential advertising cookies before consent, refusing as easy as accepting, and no cookies placed without permission. 415 passed without intervention, 564 improved after ICO engagement, 17 received preliminary enforcement notices and 21 remained non-compliant at the point of reporting. The ICO will continue testing periodically. ico.org.uk

[6] PCI Security Standards Council

The PCI DSS standard (v4.x) and the Council's applicability guidance determine actual scope; payment flows, redirection arrangements, call-centre processes and supplier relationships cannot be scoped from an external scan. Requirement 11.3.2 requires passing external scans by an Approved Scanning Vendor at least every three months and after any significant change. Under version 4 that extends to the lightest e-commerce self-assessment category, mandatory from 31 March 2025, having not applied to it under version 3.2.1. An Approved Scanning Vendor is one specifically qualified by the Council. PCI DSS standard, applicability guidance, ASV resource guide

[7] MyDomainRisk / Huro Data Technologies Ltd, four national estate baselines and one comparative baseline, updated edition, 27 September 2026, full rescan

England 314 tracked and completed, 243 exact scores (sum 18,547) and 49 floor scores (sum 3,117), 22 unscored, median 74. Wales 22 / 18 exact (1,360) / 4 floors (258) / 0 unscored, median 74.5. Scotland 32 / 19 exact (1,448) / 9 floors (577) / 4 unscored, median 76. Northern Ireland 11 / 11 exact (855) / no floors, median 76. Membership reconciles as 314 + 22 + 32 + 11 = 379 distinct websites with no cross-estate overlap. Exact scores 243 + 18 + 19 + 11 = 291, sum 22,210. Floor scores 49 + 4 + 9 + 0 = 62, sum 3,952. Published 353, sum 26,162. Averages are calculated from those underlying scores, not from rounded national averages. Exposure provenance reconciles as 4 + 2 + 5 + 1 = 12 council-level cases (10 on a database port) plus 4 on shared addresses (2 on a database port), giving 16 and 12. Of the 62 port observations, 44 belong to the council-level cases and 18 to the shared ones. The 9 September figures in the change table come from the same script run as of 13:39 UTC on 9 September 2026, which reproduces that edition exactly.

Provenance and handling

The source is one read-only production snapshot selecting the latest attempt for each tracked website; every latest attempt is dated 27 September 2026. The certificate-record reviews in section 15 were completed afterwards by queued checks and added to those attempts; they change no score. The faults in section 12 were confirmed by ordinary requests to the public addresses concerned. The extraction date does not refresh an observation, and a source date should be checked before operational use.

What this edition supersedes

This updated edition, 27 September 2026, supersedes the 9 September assessment and its 15 September revision. **Every figure here comes from the 27 September rescan; no earlier score contributes.**

Anyone holding an earlier edition should use these figures. In particular, the 9 September exposure, secure-connection, certificate and software-weakness figures have all moved, as the change table sets out, and the earlier description of why websites went unscored was wrong: most lacked only the mail transport policy.

The software-weakness evidence is described with care throughout. All 565 observations were read from software version numbers and none was confirmed by a provider; **3 entries on 3 websites appear in the actively-exploited catalogue**.

No council is named in this report. The findings are aggregate by design: a named council beside its weakness is a document that cannot safely be circulated, and the value here is the sector pattern. Per-council detail exists and is available privately to the council concerned, or to anyone it authorises.

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Every named finding should be rechecked immediately before responsible disclosure, because public-facing settings change constantly. Aggregate figures may be used with the cautions in this report. This document contains counts only: no passwords, no personal records, no raw provider data, no exploit instructions and no named council detail. A finding is not evidence that any council has been compromised or is in breach of any obligation.