The Local Gov Digital Procurement Checklist

Open Draft

A proposal for an opt-in ‘code of conduct’ for companies selling digital products and services to local government, mirroring the principles of the Local Digital Declaration. The Checklist establishes common ‘rules of the road’ for a responsible, competitive, innovative market providing digital products and services for local government.

This draft is currently being led by Open Systems Lab and Future Cities Catapult with contributions from experts and stakeholders in both private and public sector organisations. Please add your comments and

suggestions, or get in touch if you'd be interested in adopting this checklist.

Why it matters

Over the next decade, the UK aims to build world class digital local government, creating government services fit for the internet era, and levering the power of data to dramatically improve society and the economy for everyone. The cornerstones of this ambition are:

1 To design services that best meet the needs of citizens.
2 Challenge the technology market to offer the flexible tools and services we need.
3 Protect citizens' privacy and security
4 Deliver better value for money

The full vision is articulated in the Local Digital Declaration and the Technology Code of Practice

The challenge

Many of these digital tools and platforms can be built by the public sector. However, in order to be innovative, scalable, interoperable, and well-maintained across all councils, the private sector and the third sectors will also need to be involved, building new innovative digital products and services and selling them to local authorities.

This represents a particular challenge, since most companies are not there to serve the public interest; they aim primarily to maximise profits for their shareholders and if at all possible, to establish a monopoly position, or to use digital public services as a channel through which to capture citizens' personal data or to access marketing opportunities. This self-evidently prevents competition, stalls innovation, disadvantages other businesses, costs local government, erodes trust and can harm public users of government services. The market we want is one that is focused *only* on building the best possible digital public services.

The problem is that if companies **can** do these things, arguably they have little choice but to do so, since if they don't, their competitors will.

Similarly, councils are also likely to feel obligated to accept the 'cheapest' upfront deal, even if it has hidden future costs.

This is why it is in everyone's interest to have some common 'rules of the road'. Those rules or tests need to be balanced, so they create a fair, competitive market without preventing businesses from making a reasonable profit. They need to be sufficiently unambiguous tests that it is possible to know when they are not being met. Above all, they need to be simple. Technology is a complex, constantly changing area, and councils will often be too busy to think of everything that might go wrong in future. Like all good checklists, the tests need to – as far as possible – focus on core principles, indicators or outcomes, rather than specific solutions.

How to use the checklist

Like a pre-flight checklist in an aircraft, the **Local Government Digital Checklist** can be used as a kind of basic, quick 'hygiene test' for local authorities and providers. If a company or product passes the tests and is willing to carry the mark, councils can be reasonably sure that it is trustworthy, and that they are getting good value for the public.

Suppliers can use it to quickly demonstrate to prospective local government customers that their products will serve the public interest. They can also use it to hold their competitors to the same good standards.

The Checklist

Level 1 / basic

Refs	The test	What bad looks like	What good looks like
API technical & data standards ↗	**1. Services should have an open API** All digital services should have a web API that is usable and reliable, and gives other applications full ability to send data to, or request data from it. Suppliers should not unreasonably omit or refuse to include any existing data or function that would allow a safe, user-beneficial integration by others. Update: LOTI have published a superb, more detailed set of requirements for APIs here.	A supplier provides database software. Other companies would like to be able build front end services that send data to or request data from it, however its API is inaccessible, limited, inflexible and unreliable, preventing innovation.	The supplier publishes a clear, well documented and secure API for sending data to and from the database. The database defaults to an open schema, but customers can add new custom fields for no extra charge.
	2. Public data should be public Intellectual property (IP) that is inherently public such as policies, data registers, base data or standards should be freely available to everyone. Open datasets should have a named custodian who is responsible for maintaining the dataset and ensuring its integrity. Companies' business models should not seek to privately own or extract rent from data that is a necessary	A supplier is offering a platform for mapping public spatial data onto a map of a local district. However, they claim ownership of the base map, and the data is not easily transferable to another map. This gives them, in effect, a monopoly.	The supplier publishes the base map under open licence, so customers can transfer their data to another platform. The supplier competes to provide the best value platform, and benefits from others adding to the base map.

common source of truth for the whole ecosystem.

3. Personal data should be personal

The personal data of those using local government digital services should be kept private, and not sold to third parties, even where consent could be given through the Terms of Use. The exceptions to this are data that is requested and published openly (or conditionally) as part of the public record, or truly anonymised statistics or metadata, which can be published and made available (but not sold) in order to provide insight and oversight.

A supplier offers a public-facing health services platform through which members of the public interface with NHS services. They offer the software at a discounted price to customers, and instead make a profit by selling users' health data to third parties for the purpose of marketing.

The customer has to pay a higher up-front price for the service, but users health data is kept confidential and secure. It can be shared with other public sector organisations only with the user's consent.

4. No advertising

Local government digital services should not include advertising. Users of public services should be able to know that any advice they are being given is impartial, not paid-for.

A supplier provides a platform for submitting planning applications. It gives the tool to councils for free, and instead sells advertising space to local building firms. It feels a lot like Ryanair's website.

Councils have to pay for the tool, but benefit overall since it is designed to reduce their costs and make the process simple, not to maximise advertising revenue.

5. Right to data

All users, including councils, should be able to export a full, usable copy of all data or intellectual property that they have control over at no cost. This should be in a structured, standardised, machine-readable format.

A supplier provides database software. A council decides they want to transfer their data to a different system, but there is no export button. Instead, the company say there is a considerable fee to export their own data, locking them

Customer admins and users can export their data in a structured format anytime, by using an 'Export my data' button.

		in.	
	6. Easy to exit Customers should be able to exit the service without encountering ‘friction by design’. Information and reasonable assistance must be provided to exit-ing customers, enabling them to transition to an alternative service.	A customer wants to switch to an equivalent provider of a digital service. But their provider had made it deliberately difficult to do, and is slow and unresponsive; requiring written requests and demanding exit fees.	The customer can easily export their data, and simply terminate or not renew the service. If some help is needed, the supplier provides it, including liaising directly with the new supplier if easier.
	7. Inclusion by design Services should meet or exceed any published guidance, standards and best practice patterns for accessibility and inclusion. Suppliers should continuously seek feedback and to make services and content ever easier for all users to access and understand.	A supplier provides a public service job finding platform. However the interface is difficult to use for disabled users, and it is not compatible with common accessibility software, resulting in discrimination. They ignore complaints.	The supplier tests their product with a range of users and includes a feedback button. It regularly updates the product to make it more inclusive.
Making things secure↗	**8. Secure by design** Meet or exceed security best practice to prevent unauthorised access to data or systems. Don’t centralise, collect or retain any personal data that doesn’t need to be recorded for the provision of that service (or as required by law). Control who can access that data internally as well as externally.	A supplier’s mobile app allows members of the public to anonymously report antisocial behaviour. The supplier stores the device IP addresses and user location data. One of their staff looks up who is making complaints in their neighbourhood.	The supplier doesn’t collect the IP address of reporting devices. The location may be retained, it is approximated, and that data is kept securely, such that no individual staff member can access it.
	9. Seamless user experience The public should be able to use local government digital services in as joined-up way as reasonably	A supplier offers a room booking tool, that can be integrated into Council websites. However they	The room booking tool doesn’t require user login, or the two services are integrated so the

	possible, without unnecessary additional logins or barriers between proprietary applications.	require a separate username and login to be created.	user only has to log in once, if at all.
	10. Transparent All services should be as transparent as possible in how they arrive at a particular decision or result, and should log results such that they can be audited retrospectively for a minimal overhead cost. Services should make clear to users their options for recourse.	A supplier provides a tool that automates housing allocations. Users are given a result, without being able to understand the data or rules system that generated that decision, or to whom they can appeal if they feel the decision is unjust.	When a decision is issued, users can see what factors and rules were used to generate that decision, what body created them, and their options to complain.
	11. No discrimination Products and services must not discriminate against any user on the basis of gender, race, ethnicity, religion, disability, age or income, unless it is an explicit legal function of that service (for example, means testing or pensions).	A tool uses machine learning to predict rent defaults, but consistently results in a disproportionate number of warning letters being sent to a particular ethnic group.	As soon as the supplier realises or is made aware of the potential for discrimination, they no longer use it in this way.
UK Gov Open standards principles. ↗	**12. Use open standards** Third party services or datasets must use existing open standards. If an open standard does not exist, a new one should be proposed. If an open standard is inadequate, propose how it could be improved.	A supplier provides a platform for data about planning projects. However, the data is structured according to their own proprietary schema, so cannot be used by other organisations.	The company adopt a common existing schema, or creates a new one and publishes it openly for others to use and add to.
Define your purchasing strategy ↗	**13. No long lock-ins** Third party digital services should be procured as a one-off cost or on a subscription basis, with break	A council sign a 10 year contract with a supplier to develop a tool, giving them a monopoly. Once it	The council seeks innovation funding, or forms a group with other councils to collectively procure the tool in

[Agile contracting – David Kershaw↗](#)	clauses no longer than **2 years.** Wherever possible contracts should be based on usage-based billing models, ensuring fairness for smaller local authorities.	is developed, the company have no incentive to improve the tool, even as better solutions become available.	an agile way. They may then run it themselves, or have it supplied by others on a subscription basis.
[Define your purchasing strategy ↗](#)	**14. No bundling** If a company is providing multiple services in a stack (for example more than one of: server infrastructure, service integration platforms, front-end applications or data) these products must be sold separately, and priced the same as they would be to another customer buying only one of those services.	A supplier provides a poor product for an inflated price, however, the customer cannot move to an alternative because they rely on another underlying platform or dataset that is owned by the same company.	The customer can switch to another product, which also uses the same underlying platform or dataset, even though it is owned by their competitor.

Level 2 / excellent

15. Open source where possible No one should have to reinvent the wheel, or be paid to do nothing. Where functions are ubiquitous to the whole ecosystem, all parties will share the code under an open licence for others to freely use and contribute to, unless to do so would prevent them from being able to earn fair revenue, or expose customers to exploitation.	A supplier develops a piece of code for integrating their service with a gov payment service, something that many others need too. However they don't share it, so every company has to be paid to rebuild the same thing.	The supplier publishes that piece of code on Github under an open source licence, so it becomes a common solution for everyone.
16. Public Service Use license Core intellectual property (such as code) is licenced such that public sector organisations can use and	A supplier hasn't updated their product in years, but the customer	The supplier allows their Customer to use the code

improve it for free if they wish to, albeit strictly for their own use. (That is, they cannot licence it commercially or non-commercially to other public sector organisations).

still has to pay every year because the supplier owns the intellectual property.

themselves for free. This means the supplier is incentivised to keep improving the product and the service providing it.

The Checklist pass badge

The below is an idea to be explored that companies, products or services that pass these tests could carry a protected digital badge, which can be used in marketing, bidding and on the product itself.

The badge can be carried by a single product, or by the company as a whole if all their products pass the Checklist.

Who will be able to use it?

Anyone can use the checklist anytime. However, in order to get a badge or participate in the community, companies, councils and individuals will have to register.

Local authorities or departments within them can register to use the Checklist when they procure. They will be issued with a digital badge which they can use on their website, on documents or during the procurement process to demonstrate that they expect

products and services they procure to pass the Trust Check.

Suppliers can register their company or individual projects as having passed the Trust Checklist. No one checks this – it is up to them to publicly declare that they have run the checklist and their company or product passes. But their declaration is made public and visible to everyone.

They are then issued with a **digital badge** that they can embed accordingly on their website, in apps, on documents or during the procurement process to demonstrate their product(s) or service(s) are trustable.

Individuals who are passionate about great digital public services and public sector procurement can also register as an ‘independent’ supporter. This does not cost anything. Individuals cannot register as an independent if they receive money from any company that sells digital products or services to local government, or if they work for a local government. However, employees of other public sector organisations or non-profit consultants to public sector organisations can register as independent supporters.

It will not cost anything to register. However, on registering, registrants are informed that they may be called upon to do ‘virtual jury duty’ to resolve complaints.

How will it be enforced?

Generally speaking, industry self-regulation can be pretty toothless. Equally, we want to avoid the creation of an expensive regulatory body that is nonetheless still exposed to tacit capture / corruption. Instead we suggest a lean model of community / peer-to-peer enforcement:

Step 1. Raising a challenge / query

Let's say a customer or a competitor company wishes to challenge a supplier on their adherence to the standard.

They select which clause(s) they are challenging / querying and also set out their challenge or query in a paragraph. Customers and independents will have the option to remain anonymous. Representatives of companies cannot remain anonymous.

The challenge or query is then sent to the company in question, and they have 5 days to respond, by writing their own paragraph.

If the challenger is satisfied by the response, the issue is resolved.

Step 2. Taking it to a jury

If the challenger is not satisfied, they can raise a complaint.

Both the challenger and the company now have the opportunity to edit their paragraph. They are encouraged to set out the issue as concisely as

possible, and list (but not attach) any evidence they may have.

These two paragraphs are then sent in the form of a link to the jury.

The jury comprises 5 members. 2 providers, 2 customers and 1 independent. They receive a link into their inbox.

They have 48 hours to click the link, and 5 days to respond. (If they do not, the link is invalidated and sent to another equivalent juror).

As well as giving a decision, jurors may add a comment to their decision, if they want to share any explanation for how they came to their decision.

The identity of the jurors is unknown to the challenger or the company.

The decision is shared back to the parties. If the complaint was upheld the decision (and which clause(s) it applies to) is shared as part of a public record, but the content of the complaint is not. (However, the content is kept on record by the checklist maintainer in the event of any future legal disputes)

Step 3 Issuing a decision

The decision is shared back to the parties. If the complaint was upheld a record of the complaint + decision (and which clause(s) of the checklist it applied to) is shared as part of a public record, but

the content of the complaint is not. (This is kept on record though in the event of any future legal disputes)

The company's badge is revoked. This applies legally (in that they no longer have the right to use the badge to describe their product) but also practically, in that the embedded digital badge itself is automatically revoked, and will no longer display (or will display as not having passed).

Step 4 Re-adopting the checklist (tbc)
A company should have the opportunity to address the problem and re-apply in future. Obviously simply allowing them to immediately self-certify again would be absurd. However, possibly a similar process could be used whereby they can describe the changes they've made in response to the previous decision and a virtual jury approves it?

Amending the checklist

There may be a means by which the checklist can be amended in future. This could be done on a versioning / opt-in basis (like Creative Commons licences) or amendments could be approved by members votes.

Legal status

Companies and organisations that register to use the Checklist are making a statement of intent. No commercial or contractual commitment, implied or otherwise, is made by signing up to the checklist. Councils are responsible for ensuring their contracts with suppliers comply with the checklist.

However, registered signatories of the checklist are given licence to use the Checklist trademark. In the event of a challenge being upheld by a jury, that copyright / trademark licence is immediately revoked. The Checklist maintainers and juries are not responsible for any loss that results from a badge being revoked.