Dear UK Policymakers,

We, the members of ACT | The App Association, are innovative tech startups, scaleups, and independent developers driving growth and competition in the global digital economy. From AI-enabled tools, connected health solutions, encrypted services, safer online experiences, and standards-based technologies that enable interoperability, our teams build products solve everyday problems for communities and customers across the United Kingdom.

To continue building, hiring, and scaling across the global app economy, UK startups like ours need a regulatory environment that rewards innovation and provides the market certainty required to sustain investment. For small tech companies, policy volatility quickly becomes a material business constraint that shapes product roadmaps, compliance costs, and go-to-market timelines. Additionally, as roadblocks mount and timelines become harder to predict, investors view the policy environment as an additional risk that slows access to capital. That is a challenge for UK-based startups and a competitiveness challenge for the United Kingdom as a whole. A regulatory environment characterised by uncertainty weakens the innovation pipeline we rely on to lead in emerging technologies and compete globally.

As policymakers consider new rules for the digital economy, we urge balanced, forward-looking approaches that do not impose disproportionate burdens on small tech businesses. Policy should set clear expectations, provide practical paths to compliance, and deliver durable rules that strengthen trust and security while preserving the conditions that enable smaller innovators to attract investment and compete. Below is an outline of our top policy priorities for UK leadership in 2026.

Artificial Intelligence

For startups and small tech businesses, the UK's AI policy choices will determine whether building and scaling AI products remains practical or becomes a compliance exercise only the largest firms can absorb. The AI Opportunities Action Plan sets out an agenda to grow the AI economy through new growth zones, expanded computing capacity, and a National Data Library to unlock new AI applications across the public and private sectors. But flexibility only helps if expectations are clear. When guidance is inconsistent across regulators or shifts mid-development, smaller teams are forced into rework and guesswork, which slows deployment and increases costs.

> **Member Ask:** UK policymakers should coordinate and simplify AI oversight, so compliance expectations are consistent, predictable, and proportionate for startups and independent developers.

Mergers and Acquisitions

Mergers and acquisitions are a core way for UK founders to turn successful products into the next iteration of innovation, as many founders build, exit, and reinvest to start new innovative

companies. When merger control is unclear or feels like a moving target, that uncertainty shows up long before any deal is on the table. It changes how investors price risk, how boards plan timelines, and whether scaling in the UK looks financeable in the first place. The CMA's Mergers Charter is a welcome step toward restoring confidence by committing to pace, predictability, proportionality, and a fair process, including clearer signals on when the CMA is likely to review a transaction.

> **Member Ask:** Apply the Mergers Charter in practice by giving clearer jurisdictional guidance early, keeping information demands proportionate, and running reviews at pace so pro-competitive deals are not delayed by avoidable uncertainty.

Competition and Curated Online Marketplaces

Curated online marketplaces (COMs) are a primary route to market for startups and independent developers in the UK, and the trust consumers place in these marketplaces is essential to competing on quality and security. Under the Digital Markets, Competition and Consumers Act (DMCCA), the Competition and Markets Authority's (CMA's) proposed roadmaps for mobile ecosystems will shape how smaller innovators can build, distribute, and scale. We appreciate the CMA's pause on proposals that would require access for third-party app stores and sideloading, which recognises the potential harm alternative app distribution can pose to consumer security and trust. Significant issues remain, including proposed AI and interoperability interventions that could introduce new security risks and reduce access to the tools and infrastructure developers rely on, such as privacy protection, data security, and subscription management, which help offload overhead and enable even small teams to reach customers globally.

> **Member Ask:** The CMA should implement the DMCCA with clear, consistent, technically-grounded roadmaps that prioritise user security and trust and reflect how smaller developers depend on curated marketplace protections, ensuring interventions do not end up delivering the biggest gains to a handful of large firms while raising cost and complexity for the wider developer ecosystem.

Digital Trade

The UK's growth in the global digital economy depends on frictionless digital trade with key partners. The 8 May 2025 U.S. – UK trade agreement signalled momentum and was framed as a springboard for a deeper technology partnership, including emerging areas like AI and quantum and efforts to simplify trade for digital-first businesses. However, the deal was light on the fundamentals that determine whether smaller firms can scale across the Atlantic, including clearer commitments on reducing regulatory divergence, protecting cross-border data flows, and addressing unresolved questions in the UK's digital policy environment such as the Digital Services Tax. When those issues stay unsettled, the burden lands first on smaller teams through higher compliance overhead, slower partnerships, and a less predictable path to grow internationally.

Member Ask: Policymakers should build on the momentum by locking in practical digital trade outcomes that work for smaller firms, including stronger alignment to reduce cross-border friction, durable protections for cross-border data flows, and a clear approach to UK digital policy issues that shape market access and investment confidence.

Standard-Essential Patents (SEP)

Standards for interoperability and safety provide a baseline for competition and innovation across consumer and enterprise markets. As small tech companies increasingly innovate in rapidly advancing fields like AI and the internet of things (IoT), many are not only implementing standards, but also contributing to the next generation of standardized technologies.

When standards include patented technology and the standard cannot be used without exercising the patent, they become standard-essential patents (SEPs). Because SEP holders are inherently positioned as arbiters of who can and cannot use the standard, standards bodies require those choosing to contribute their patents to a standard to license them to all on fair, reasonable, and non-discriminatory (FRAND) terms. A licensing framework that advances transparency, fairness, and predictability by ensuring that FRAND promises are kept is therefore crucial for ensuring small businesses can indeed use standardized technologies to interoperate and compete.

The UK's current SEP licensing environment is still opaque and unpredictable for smaller teams, with costs and exposure often unclear until late in development and negotiations that can feel driven by leverage rather than the FRAND licensing process. The UKIPO's recent work, including its consultation and proposals to streamline rate-setting, is a step in the right direction, but reform only helps if it delivers real transparency, credible guidance, and a system that reduces litigation pressure rather than merely reallocating it.

Member Ask: Policymakers should ensure UK SEP reform produces predictable outcomes in practice by improving transparency and information symmetry, establishing clear aggregate royalty benchmarks, creating accessible FRAND guidance for smaller teams, requiring standardised disclosures in licensing demands, and making clear that injunctions for FRAND-committed SEPs should be exceptional, not a negotiating tool.

Online Safety

We support measures that protect children online from privacy violations and harmful content. However, attempts to weaken encryption using the Investigatory Powers Act and enforcing age verification methods under the Online Safety Act are inadvertently putting children at a greater risk.

Enforcement includes forcing developers to implement intrusive checks that collect identity and sensitive personal data. For startups and independent developers, this turns product teams into

identity and high-risk data custodians overnight, pushing services toward IDs, facial images, or behavioural signals that expand breach risk and increase the real-world harm users face when systems fail, as the "Tea breach" made painfully clear. Systems that are costly to build and maintain, and easy to bypass in practice do not provide safety, only increase risk.

End-to-end encryption underpins trusted digital services, from messaging and collaboration tools to payments, health platforms, and safety features built into everyday apps. Proposals arising from the implementation of the Online Safety Act that favour client-side scanning or other forms of privileged access would weaken that foundation by introducing new breach opportunities, increasing the risk of fraud and abuse. Both these and the age verification requirements would disproportionately affect smaller teams. Large incumbents can absorb redesign costs and liability exposure brought by these rules, but smaller teams often cannot, forcing them to choose among weakening security, limiting features for UK users, or exiting the market.

> **Member Ask:** UK policymakers and Ofcom should protect children without normalising surveillance. That means avoiding default expectations for ID and biometric-based age checks and prioritising privacy-preserving approaches that minimise data capture and retention. Additionally, it is critical policymakers protect strong end-to-end encryption by rejecting client-side scanning, backdoors, or exceptional access, with clear, scalable, and proportionate guidance that smaller firms can actually meet.

Innovation thrives when policymakers create clear, durable rules that allow businesses of all sizes to compete and succeed. Overly broad, fragmented, or unpredictable requirements raise compliance costs, delay product development, and undermine the investment that small tech businesses need to grow. We remain committed to working with parliamentarians, regulators, and the wider tech ecosystem to advance these priorities and ensure that small tech can continue to create jobs and deliver practical solutions in the global digital economy.

Sincerely,

ACT and our members