

OPEN RIGHTS REPORT AND ACCOUNTS

YEAR ENDED 1 JANUARY 2025 TO 31 DECEMBER 2025



Publicity stunt conducted
by the Safety Not Surveillance
coalition in central London

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. We are a grassroots organisation with supporters and local groups across the UK.

Our work on data protection, privacy and freedom of expression includes: challenging harmful pre-crime programmes such as Prevent; campaigning for the digital rights of migrants, including through legal challenges to the immigration exemption in UK data protection law; fighting to protect end-to-end encryption; and campaigning against uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

COMPANY INFORMATION

For The Year Ended 31 December 2025

Directors
Sandeep Gopalan
Luisa Porritt
Adela Devlin
Gregory Mayne
Melanie Harper
Christian Scarborough
Steven Murdoch
Anna Fielder
Hannah Little
Edward Bridges

Registered Office
Space4 113-115 Fonthill Road
London
N4 3HH

Accountants
Urban Ledgers Limited
124 City Road
London
EC1V 2NX

Company number
5581537

Published under a Creative Commons
Attribution-ShareAlike 3.0 Unported Licence
<https://creativecommons.org/licenses/by-sa/3.0/>
except where stated.



ANNUAL REPORT OF THE DIRECTORS

OUR OBJECTIVES, MISSION, AND ACTIVITIES 1

CHAIR’S FOREWORD 2

INTRODUCTION 4

PLATFORM POWER 6

HOLDING THE ICO TO ACCOUNT 6

ADTECH 8

DATA AND DEMOCRACY 9

ONLINE SAFETY ACT 9

BLOCKED.ORG.UK 11

ENCRYPTION 11

MIGRANT DIGITAL JUSTICE PROGRAMME 12

STRENGTHENING OUR NETWORK 12

CAMPAIGNING AGAINST EVISAS 12

PRE-CRIME 14

CHALLENGING PREDICTIVE POLICING 14

INVESTIGATING THE DIGITAL HARM OF THE PREVENT DUTY 14

SUPPORT OUR WORK 15

ACCOUNTANT'S REPORT 16

REPORT OF THE BOARD OF DIRECTORS

The Directors of the company present their annual report for the year ending 31 December 2025.

The Directors would like to thank our members, supporters, donors and grantors, who made our important work possible. The Directors would also like to thank our staff, volunteers, members of our local groups and Advisory Council for their hard work, support and world-class expertise.

OUR OBJECTIVES, MISSION, AND ACTIVITIES

The World We Want

A world where technology supports justice, rights and freedoms to prevail over powerful monopolistic interests; and neither states nor corporations use digital technology to restrict, monitor or control people.

The problem we face

People's rights are systematically undermined by:

- Expanding state surveillance across policing, welfare and immigration.
- Corporate concentration of power, especially in cloud, AI, adtech and communications infrastructure.
- Digital dependency risks, where government and society rely heavily on foreign tech vendors, opaque systems, and outsourced policy promoted by tech vendors
- AI-driven profiling and discrimination, disproportionately targeting marginalised communities, who are often used as a vanguard for rights reducing tech.
- Regulatory instability and weakened data protection.
- Political volatility, leading to scapegoating marginalised communities, authoritarianism and rights erosion, collision of tech corporate interests with authoritarianism.

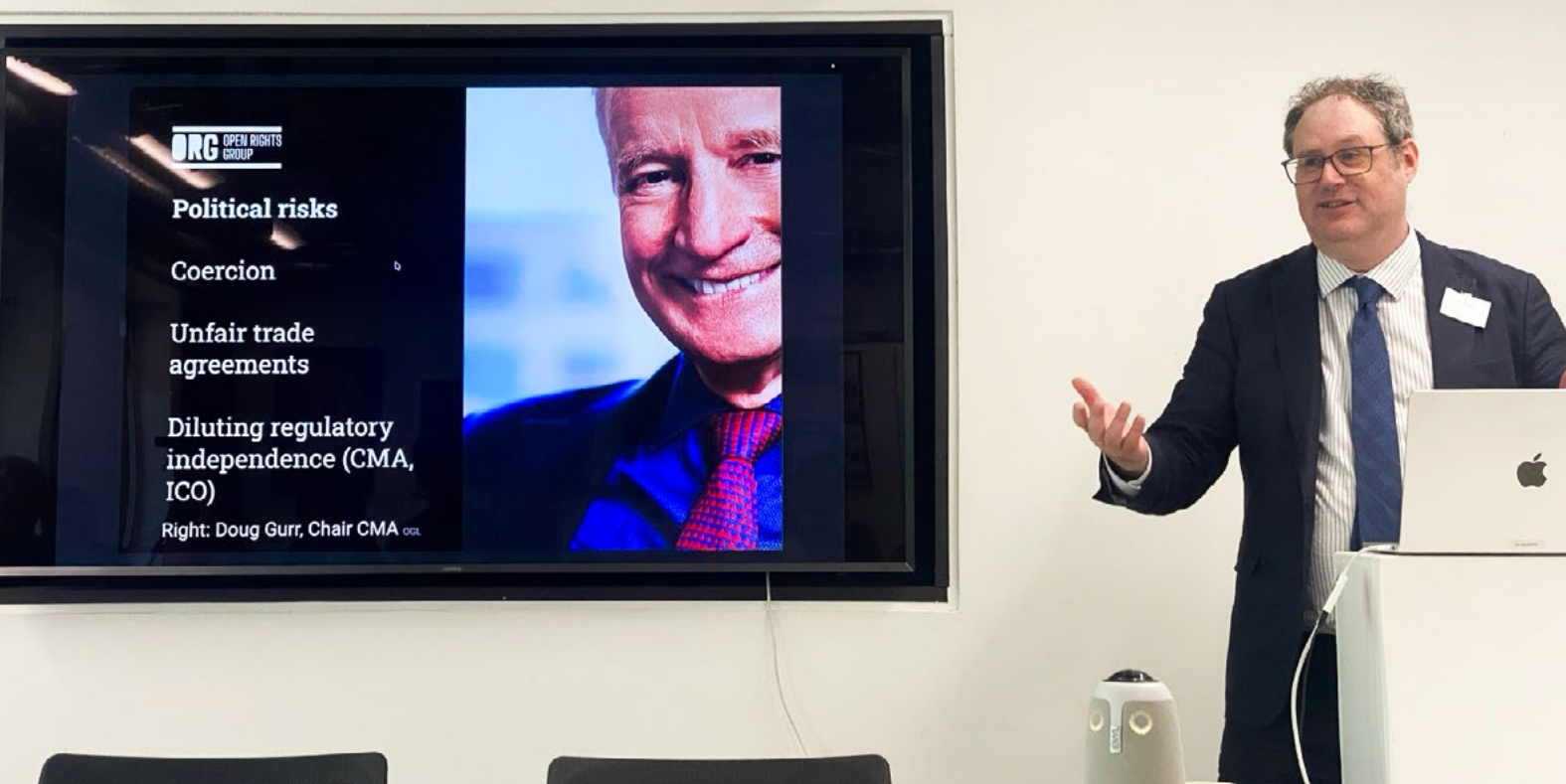
These forces entrench inequality and reduce rights and their democratic underpinnings. They also generate new opportunities to push back through new forms of political opposition.

The Impact We Seek

We want to create free and democratic environment where politicians, civil society and the general public are well informed and equipped to ensure that technology is directed to protect and promote human rights and social justice. We want to learn from and work with communities most affected by digital harms, to ensure decision-makers understand the consequences of unaccountable Big Tech, a Pre-Crime state and a Digital Hostile Environment.

The Values that Guide Us

- We believe **digital rights are human rights**.
- We want to help build an **equitable and just society**.
- We work **collaboratively**, building **collective knowledge and power**.
- We are **accountable** to our supporters, society and allies, and operate with **integrity and transparency**, holding ourselves to the standards we expect of others.
- We are **flexible, adaptive and evidence-based**.



ORG's Executive Director, Jim Killock, explains the harms of digital dependency at Sussex University's Digital Sovereignty event

How We Work

We uphold digital human rights such as free expression and privacy. We condemn and work against repressive laws or systems that deny people these rights. We seek impact working to defend rights and correct injustice.

- We DEFINE harms and abuses through our research and investigation.
- We PERSUADE allies and adversaries through our policy advocacy especially in Parliament.
- We BUILD alliances with those most directly impacted when rights are undermined.
- We MOBILISE with those directly impacted, with our members and supporters across the UK through our public campaigns.
- We CONFRONT threats to our fundamental rights through our litigation.
- We campaign, lobby, go to court – whatever it takes to build and support a movement for freedom, rights and justice in the digital age.

CHAIR'S FOREWORD

2025 was a year in which the influence of technology over our lives, politics and public services was central to social and political debate. Across government, business and society, digital systems are presented as solutions to complex social and economic challenges. Too often these technologies are deployed without adequate safeguards, accountability or regard for the rights and freedoms of the people they affect. Whether they are even real solutions for the problems they seek to address is often doubtful. What is clear is that tech solutionism is good for tech businesses and provides politicians with claims of action, while more often than not, creating systems of surveillance, censorship and control, in place of genuine social remedies.

Open Rights Group continued to play a vital role in defending privacy, free expression and democratic accountability.

Throughout the year, we challenged the implementation of the Online Safety Act, highlighting its impact on freedom of

expression, access to information and the viability of smaller online communities. As age-verification requirements came into force, we documented their unintended consequences, provided practical guidance to organisations and users, and developed constructive proposals for reform.

We also stood firmly in defence of encryption and secure communications. When government efforts threatened the security of encrypted services used by millions of people, ORG helped ensure these issues received public scrutiny and mobilised widespread support for the principle that privacy and security are fundamental rights, not obstacles to safety.

Our work on data protection and platform accountability remained at the forefront of national debates. We challenged regulatory failures, scrutinised attempts to weaken data protection standards and continued our efforts to expose the harms caused by surveillance-based business models. Through research, advocacy and coalition-building, we helped ensure that the voices of citizens and civil society were heard alongside those of governments and technology companies. Data protection is currently a national disgrace. Online Safety delivers little and harms more. ORG is a vital voice helping explain what Online Safety could really be, by pushing back the power of tech giants.

The year also saw significant progress in our Migrant Digital Justice Programme. This is an area where tech solutionism is hard at work. Collaborating closely with migrant communities and partner organisations, we exposed the harms caused by the UK's eVisa system and highlighted the risks of digital identity systems that exclude, discriminate and deepen inequality. Our research and campaigning brought the experiences of affected communities directly into public and political discussions.

At the same time, we expanded our work challenging predictive policing, facial recognition and other forms of data-driven surveillance. Through the growing Safety Not Surveillance coalition, we worked alongside community groups, campaigners and

experts to push back against technologies that risk embedding discrimination and undermining fundamental democratic principles. This is a genuine grassroots pushback, mobilising those most at risk, and bring their voices together with technologists and political power.

What unites all of this work is a simple belief: technology should serve people, not control them. Whether challenging surveillance, defending encryption, protecting migrants' rights or promoting accountability for powerful institutions, ORG's role is to ensure that human rights remain at the centre of decisions about our digital future.

None of this would be possible without the commitment of our staff, volunteers, members, supporters, donors and partner organisations. Their expertise, energy and determination enable us to confront some of the most important challenges facing our society.

As we look ahead, the pressures on rights and freedoms in the digital world show no sign of diminishing. The environment is extremely challenging, but we continue to stand as a voice for human rights and effective rather than knee-jerk digital policy making in a deeply divided world. Open Rights Group enters the coming year stronger, more connected and more committed than ever to ensuring that technology advances justice, freedom and democracy for everyone.

Hannah Little

Chair, Open Rights Group.



ORG's Alberico Ricci hosting an ORG supporters' event at Newspeak House in London

INTRODUCTION

2025 marked another year of Big Tech's ever-increasing influence in politics, with AI at the forefront of public debate. Economic pressures continued to drive rapid digitisation across both the public and private sectors, and AI was lauded as a solution to stagnant productivity and overstretched public services. Against this backdrop, Open Rights Group stood firm as a voice for privacy, free expression, and the rights of the most vulnerable in our society.

This was the year the Online Safety Act came into force, and with it, a wave of unintended consequences that bore out many of ORG's longstanding concerns. Internet users across the country found themselves compelled to hand over personal data to unregulated age-verification companies simply to access content and app features, extending far beyond the stated aim of protecting children

from harmful material. Our monitoring revealed that health advice, educational resources, and content relating to Palestinian solidarity was swept up in age-gating measures, demonstrating how overly-broad legislation stifles access to legal information. Small websites and community forums faced impossible compliance burdens, with many shutting down or geo-blocking UK users entirely rather than risk exorbitant and punitive fines. Alongside our partners, ORG called for the age-verification industry to be properly regulated to minimise risk to users. Throughout the year, we tracked this creeping censorship, published guidance for organisations grappling with the Act, and released a major report,¹ "How to Fix the Online Safety Act", setting out a rights-based approach to fixing its most damaging provisions. Our subsequent interoperability

¹ <https://www.openrightsgroup.org/publications/how-to-fix-the-online-safety-act-a-rights-first-approach/>

report² made the case that genuine online safety requires structural change: empowering users to choose their own content moderation and switch providers without losing their networks, rather than entrenching the dominance of Big Tech.

Throughout the year, we continued to defend encryption and secure communications. Both the Online Safety Act and the Investigatory Powers framework intensified the pressure on security measures, with both leaning into the narrative of protecting citizens. The prospect of mandatory message scanning and government demands for exceptional access to private communications threatened the security of millions of users. Open Rights Group's "Practice Safe Text" campaign helped bring public attention to the importance of end-to-end encryption not only for journalists, activists and vulnerable groups, but for everyone who relies on secure digital services in daily life. We also highlighted the potential damage that could be caused by proposals to restrict or age-gate VPNs, given how these tools are essential for security, privacy, and free expression. Our advocacy helped strengthen public understanding that weakening encryption does not create safety, but puts us all at risk.

Equally, when the government sought to force Apple into providing backdoor access to encrypted communications, ORG intervened decisively. Working with lawyers and technologists, we fought to ensure that at least part of Apple's appeal would be heard in public, recognising the global implications of such a precedent for secure communication. Although the government reportedly backed down from forcing Apple to compromise its own security, we anticipate that future governments will continue to try to erode these protections.

The Home Office's flawed eVisa scheme presented us with another ill-conceived piece of tech-policy. Throughout the year, we heard from migrants left unable to prove their right to live and work in the UK, with devastating

consequences: job offers withdrawn, university places lost, and, in some cases, homelessness. Our advocacy secured a delay to the scheme's original deadline, buying time for further investigation of the scheme and giving the Home Office the opportunity to mitigate the most egregious issues. We shared our findings with a number of migrant rights organisations and legal partners, and published joint research with Migrant Voice and academics from the University of Warwick and the University of Leicester, which exposed the emotional and practical toll of the scheme.

In the Autumn of 2025, there were renewed proposals for a digital ID scheme in the UK. The proposal evolved with time, shifting from an opt-in model for certain demographics to a mandatory system for all working British citizens. There was overwhelming public backlash, with nearly 3 million people signing a parliamentary petition opposing digital IDs, and support for the scheme collapsed to 15% after organisations like ORG raised our concerns.

In line with the government's ever-growing appetite for surveillance, the increasing use of predictive policing tools brought about much for ORG to challenge. Now used by 75% of police forces across the country, these tools and data-driven systems risk entrenching bias, eroding public trust, and undermining the presumption of innocence. In November, we took our concerns directly to the National Police Chiefs' Conference, challenging the normalisation of surveillance tools that treat communities as suspects rather than citizens.

We expect to face expanding surveillance and digital control in the coming years, but are buoyed by the determination and dedication of our staff, volunteers, donors, and—above all—our members and supporters. Together we will fight to advance our digital rights and push back against creeping authoritarianism.

² <https://www.openrightsgroup.org/publications/making-platforms-accountable-empowering-users-and-creating-safety/>

PLATFORM POWER

The UK has shifted away from the European model of data protection, and is now implementing changes that will relax restrictions around how personal data can be used. At the same time it is increasing online safety duties and regulations. These new safety duties have quickly become an opportunity and a legal basis for online surveillance, as well as creating freedom of expression issues and new market access barriers for small community sites.

Holding the ICO to account

The Information Commissioner's Office (ICO) has a poor track record of enforcing data protection law, issuing weak reprimands instead of fines and being overly-lenient to government bodies who leak citizens' data. In 2025, we continued to hold the regulator to account and raised awareness of its poor track record with the public and decision makers.

In May we worked with Siân Berry MP to table an amendment to the Data Use and Access Bill to introduce a statutory complaints procedure for people in vulnerable situations, along with a right of appeal to the Information Tribunal. Given the heightened risk for many people facing violence, any information that can reveal the habits or whereabouts could put them and their children at risk of harm. We called for a mechanism facilitating expedited complaints from people who are vulnerable, e.g. fleeing modern slavery or domestic violence, if companies and organisations have failed to protect their data adequately.

In June we worked with EDRi to mobilise European civil society organisations to write an open letter to European Commissioner, Michael McGrath, over concerns about the erosion of privacy and data protection in the UK.³ The letter questions the legitimacy of the adequacy agreement with the UK under EU GDPR, given the UK's sustained and

systemic divergence from the EU's position on strong data protection. Together with the EDRi Bruxelles Office, we followed up with a series of meetings with EU Commission officials, as well as letters for EU Member States representatives, national Data Protection Authorities, the European Data Protection Supervisor and the European Data Protection Board. As a result, the UK adequacy decision was amended to include a section that establishes a reinforced monitoring mechanism. This can be used by the European Commission to monitor the UK government's use of delegated legislative powers to amend UK data protection law, as well as the performance of the ICO and practical interpretation they will adopt. Under this new mechanism, the Commission would issue the UK government with a three-months advanced notice if there were "developments" that warrant an amendment, suspension or repeal of the adequacy decision.⁴ This is an unprecedented mechanism, which came as a direct application of ORG's recommendation to strengthen monitoring mechanisms within the adequacy determination.⁵

In September the ICO launched a consultation on its new complaints handling procedure. This new procedure would essentially establish their failure to investigate complaints correctly as a policy where they only action certain strategic or key complaints issues. ORG responded to this highlighting it might result in the ICO failing to fulfil its statutory duties.⁶ We also shared a template response to the consultation with data protection experts and other interested parties. As a result, the ICO response to the consultations' findings had to acknowledge widespread disagreement regarding their

proposals.⁷ This acknowledgement is particularly important since ORG has, in cooperation with the Good Law Project, sent a pre-action letter to the ICO, as the first step to raise a judicial review against the new complaints policy.⁸

In November, in light of a number of high-profile ICO failings, including the decision not to investigate the Afghan data breach where the details of over 19,000 people fleeing the Taliban were leaked, we mobilised over 70 organisations and experts in a joint open letter.⁹ Together, we urged the Chair of the Select Committee for Science Information and Technology to open an inquiry into the collapse in enforcement activity by the ICO. This led to her acknowledgment that the ICO response to the breach "paint a clear picture of institutional failure".¹⁰

Though the Afghan data breach was one of the most serious in British history, it is not an isolated case. Evidence shows a correlation between the ICO's lack of formal regulatory action and a surge in, sometimes egregious, data breaches in the UK. This was evidenced again in December, when the ICO issued a reprimand to the Post Office for their Horizon IT scandal data breach, unlawfully publishing the identities of Horizon's victims, rather than fining or prosecuting those responsible. Our work was covered in The Guardian,¹¹ The Register,¹² and Computing UK.¹³

⁷ <https://ico.org.uk/about-the-ico/responses-to-ico-consultations/summary-of-responses-to-the-ico-consultation-on-draft-changes-to-how-we-handle-data-protection/>

⁸ <https://goodlawproject.org/were-challenging-the-ico-for-ignoring-thousands-of-data-complaints/>

⁹ <https://www.openrightsgroup.org/press-releases/70-organisations-and-experts-demand-action-over-failing-ico/>

¹⁰ <https://committees.parliament.uk/publications/50560/documents/275905/default/>

¹¹ <https://www.theguardian.com/technology/2025/nov/24/civil-liberties-groups-call-for-inquiry-into-uk-data-protection-watchdog>

¹² https://www.theregister.com/2025/11/25/ico_inquiry_afghan_mod/

¹³ <https://www.computing.co.uk/news/2025/legislation-regulation/rights-groups-accuse-ico-of-collapse-in-enforcement-activity>

Adtech

We have been raising awareness and challenging the use of 'Real-Time Bidding' systems to gain access to personal data for targeted advertising. From highest to lowest bidder, personal data is harvested and combined with other datasets to build a profile about each individual. Everything from geolocation, political beliefs and sexual preferences to your browsing habits and information about your devices come under the hammer. This work has involved hosting events, pushing the ICO on enforcement, and filing complaints.

In 2025 we also supported litigation brought by tech expert Tanya O'Carroll against Meta.¹⁴ In the case, O'Carroll argued that Facebook's targeted advertising system was covered by the UK's definition of direct marketing, giving individuals the right to object and Meta settled in March 2025.¹⁵ To raise awareness of the real life harms of stalker advertising, we conducted research into how Meta monetised the migrant crisis,¹⁶ how its model fuels discrimination and preys on people's vulnerabilities.¹⁷ Moreover, we ran a public stunt outside Meta's offices pushing for compliance with the ruling. The day after we published our film of the stunt, people began to receive responses, albeit unsatisfactory ones, as they have not been fully opted out of targeted advertising. Furthermore, we have designed a simple opt-out tool for Meta users, which over 500 people used,¹⁸ as well as supporting individuals to bring complaints to the ICO. Meta has since switched to a 'consent or pay' model, which we argue must still allow users opt out of stalker ads, as contextual adverts could be leveraged instead.¹⁹

¹⁴ <https://www.bbc.co.uk/news/articles/c1en1yvjv4dpo>

¹⁵ <https://techcrunch.com/2025/03/21/meta-settles-u-k-right-to-object-to-ad-tracking-lawsuit-by-agreeing-not-to-track-plaintiff/>

¹⁶ <https://www.openrightsgroup.org/press-releases/new-report-how-meta-is-monetising-the-migrant-crisis/>

¹⁷ <https://www.openrightsgroup.org/press-releases/meta-requires-more-transparency-about-anti-gambling-ads-than-gambling-ads/>

¹⁸ <https://action.openrightsgroup.org/meta-opt-out>

¹⁹ <https://www.openrightsgroup.org/press-releases/metass-consent-or-pay-must-not-allow-stalker-ads-report-argues/>

³ <https://edri.org/our-work/uk-data-adequacy-under-scrutiny-civil-society-warns-eu-not-to-reward-deregulation-disguised-as-simplification/>

⁴ https://commission.europa.eu/document/download/a7907f8f-6e1c-4782-a193-d16b2cfe7650_en?filename=JUST_template_comingsoon_standard_26.pdf (page 35)

⁵ <https://www.openrightsgroup.org/publications/draft-uk-adequacy-decision-summary-of-findings/> (Section 12)

⁶ <https://www.openrightsgroup.org/publications/org-response-to-consultation-on-the-icos-approach-to-data-protection-complaint-handling/>



Public stunt in support of litigation against Meta, enforcing the Right to Object under GDPR

ORG has also been participating in the advertising harms sub-group of the Online Safety Act Network. This work has been helping to bridge understanding between safety campaigners and digital rights campaigners around the relationship of surveillance advertising and online harms. A joint letter was signed by ORG and a number of safety campaigners that including points around the right to object to targeted advertising, and the consent or pay model adding to online harms.

Finally, ORG engaged with the ICO consultation on a new approach to regulating online advertising.²⁰ We emphasised that the new approach would remove important legal safeguards against online surveillance and predatory or discriminatory

advertising. We also convened a round table with the ICO, DSIT, civil society organisations, data protection experts and privacy-preserving adtech providers.²¹ The ensuing report pushed back against the ICO's plans, exposing government interference in the ICO, as well as the irrationality of the ICO's proposed position not to enforce legal requirements. As a result, the ICO's statement has been significantly delayed: initially meant to be issued in early 2026, it is still not published at time of writing. Furthermore, the ICO accepted that the statement will only serve as a recommendation to government, and would not be immediately implemented by the ICO through amendments to their enforcement policy.

²⁰ <https://www.openrightsgroup.org/publications/org-response-to-ico-call-for-views-on-our-approach-to-regulating-online-advertising/>

²¹ <https://www.openrightsgroup.org/publications/notes-from-org-adtech-roundtable-on-the-future-of-cookie-consent-requirements-in-the-uk/>



James Baker, ORG's Platform Power Programme Manager, at the Labour Party conference's Campaign Fringe

Data and democracy

We published our report, *Moral Hazard: Voter Data Privacy and Politics in Election Canvassing Apps*, in January this year.²² The report raises concerns about the privacy and security of canvassing apps used by political parties. The report also found that there is a lack of transparency over how data is used, which also raised the question of whether voters' data is being used unlawfully.

The findings in our report were even more critical given the implications of the Data Use and Access Bill. The Bill includes provisions to give the Secretary of State powers to change the rules around how data can be used without parliamentary scrutiny. It opens up the possibility of a government minister using these 'Henry VIII' powers close to a General Election, in ways that could favour the political party in power. We mobilised democracy organisations, privacy groups and academics to warn government ministers that these powers could threaten the integrity of future elections.

²² <https://www.openrightsgroup.org/press-releases/new-report-voter-data-privacy-concerns-over-apps-used-by-political-parties/>

Online Safety Act

In 2025, the Online Safety Act (OSA) came into force. Applying to any online service that enables users to post content or interact with others, which includes everything from Reddit to Spotify, the OSA has forced Internet users to hand over personal data to unregulated age-verification companies just to access content and app features. Ostensibly to protect kids from seeing harmful content online, there have been a number of unintended consequences, as ORG warned there would be. The topics limited by the Act go well beyond porn, with health advice and content about Palestine being age-gated. Many community websites and message boards have chosen to shut down completely rather than risk crippling fines for breaching the rules. We argued that rather than making the internet safer, the OSA instead entrenches Big Tech's market dominance, as only the biggest platforms can afford to take the financial risk of punitive fines.

We continued to challenge this legislation throughout the year. We tracked the creeping censorship the OSA caused, securing widespread press coverage on how the Act would limit conversations around non-violent direct action and Palestinian solidarity,

including in The Guardian²³ and The New Arab.²⁴ We issued guidance²⁵ to organisations navigating the Act, including which sites would fall into purview and explaining the new duties placed upon them. We worked with a number of grassroots groups impacted by the Act, including those involved in Palestinian solidarity, sex work, racial justice and LGBTQIA rights and put together a policy hub to share our research and campaign actions.²⁶ We also published a major report exploring how the OSA can (and must) be fixed.²⁷ This report has been viewed over 3,000 times.

Alongside our opposition to the chilling effect of the OSA on public discourse, we also opposed unregulated age-verification providers. We united organisations to demand better regulation of the age-verification sector and warned the public, MPs and regulators of the privacy and cybersecurity risks posed by leaks of sensitive data required to verify people’s age. To support people navigating age-verification, we launched a website²⁸ to share information with adults, children and website owners and engaged a number of news outlets, including The Huffington Post,²⁹ BBC³⁰ and Politico.³¹ Rather than playing whack-a-mole with harmful content, our interoperability

report³² put forward a case for disrupting the attention-market through existing competition powers, so that users can choose their content prioritisation and moderation engines.

In June Ofcom launched a 309 page consultation (plus annexes) on additional safety measures. ORG responded to this consultation raising a number of concerns about restrictions on livestreaming, and proposals to expand perceptual hash matching for terrorist, and intimate image abuse content to a wide variety of online services.³³ In addition we ran a campaign highlighting the consultation that resulted in 204 of our supporters engaging and submitting their own responses.³⁴

In September ORG produced a briefing document around VPNs and the OSA.³⁵ This document was produced in response to Parliamentary and media concern that VPNs were being used to circumvent the age-gating measures the Online Safety Act requires platforms to implement.

Working with Bird & Bird, ORG drafted an amendment to the OSA that would exempt small sites from falling under its scope. We presented this amendment to Online Safety Campaigns, and digital rights campaigns at a roundtable, and met with DSIT officials to discuss whether it could be implemented. As of yet we have been unable to get this amendment tabled in Parliament.

In December, ORG worked with MPs during their debate on a petition to repeal the OSA. A number of MPs raised the issue of small sites being forced to close by the OSA, despite the majority clearly being in favour of retaining all the powers contained within the Act.

Blocked.org.uk

Mobile and broadband Internet Service Providers (ISPs) have created filters to stop under-18s from seeing online content that is intended for adults. Unfortunately, filters block many harmless websites by mistake – even sites that are aimed at children. Often website owners are unaware that this is happening.

Our Blocked.org.uk tool continued to help users find out if a website is blocked by their Internet service provider, by mobile content filters or by a court-ordered block. Our service also helped users file requests to get sites unblocked. Our tool identified thousands of sites that remained blocked in 2025, including charities offering support for substance abuse, mental health, domestic violence and LGBTQ+ issues.

In 2025 we upgraded the Blocked site to include a functionality for people to record sites that have closed or started geo-blocking the UK in response to the Online Safety Act.

Encryption

In 2025, the Home Office served Apple with a Technical Capability Notice under the Investigatory Powers Act 2016. The Technical Capability Notice would force the company to build a backdoor into their end-to-end encrypted iCloud services. Recognising the impact this could have on thousands of Apples customers in the UK, and the huge global implications for secure communications more broadly, ORG stepped in. We organised a joint letter with Big Brother Watch, Index on Censorship, and other key rights groups to the President of the Investigatory Powers Tribunal, the Rt Hon Lord Justice Singh, and successfully fought to ensure that at least some of Apple’s appeal would be heard in public.³⁶

With help from our supporters, we worked with lawyers to make sure the perspective of technologists and privacy services, alongside their users, would be put forward in that case. We secured over 2,000 signatures on a petition calling for the Government to rescind this demand,³⁷ ran a crowdfunding campaign raising £5,000 to support our activities, as well as compiling an amicus curiae brief with the help and input of corporate supporters and partners. Our work to push for transparency for this case received widespread press interest, with articles in the BBC,³⁸ Washington Post,³⁹ FT⁴⁰ and others. Although the government has now backed down on forcing Apple to break its own security, the dangerous powers that enabled them to call for this backdoor remain part of Investigatory Powers Act. We will continue to fight these assaults on security and privacy.

Alongside our work on the Apple case, we ran our Practice Safe Text campaign⁴¹ to underscore why encryption matters for us all. We explained how vital encryption is to children who want to keep their communications secure from online predators and stalkers, not to mention journalists, whistle-blowers, parents, domestic violence victims and the LGBTQ+ community,⁴² all of whom rely on encrypted services to find community, resources and support.

23 <https://www.theguardian.com/world/2025/aug/02/palestine-action-ban-coupled-with-online-safety-act-are-threat-to-public-debate>

24 <https://www.newarab.com/news/uk-legislation-serious-attack-gaza-debate-rights-groups>

25 <https://www.openrightsgroup.org/publications/online-safety-act-a-guide-for-organisations-working-with-the-act/>

26 <https://www.openrightsgroup.org/campaign/online-safety-bill-campaign-hub/>

27 <https://www.openrightsgroup.org/publications/how-to-fix-the-online-safety-act-a-rights-first-approach/>

28 <https://www.ageverificationfacts.org.uk/>

29 https://www.huffingtonpost.co.uk/entry/porn-age-verification-check-advice-parents_uk_6881ea8de4b0d55a3f196462

30 <https://www.bbc.co.uk/news/resources/idt-bfe8d0c8-c977-483c-a074-c15fafb654e8>

31 <https://www.politico.eu/article/britain-mps-charge-vpns-expenses-minister-caution-tech-jonathan-reynolds-data/>

32 <https://www.openrightsgroup.org/publications/making-platforms-accountable-empowering-users-and-creating-safety/>

33 <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-online-safety---additional-safety-measures/responses/open-rights-group.pdf?v=409223>

34 <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-online-safety---additional-safety-measures/responses/open-rights-group-campaign.pdf?v=409222>

35 <https://www.openrightsgroup.org/press-releases/new-briefing-warns-against-restricting-vpns/?hl=en-GB>

36 <https://www.openrightsgroup.org/press-releases/make-the-investigatory-powers-tribunal-on-apple-encryption-a-public-hearing/>

37 <https://you.38degrees.org.uk/petitions/keep-our-apple-data-encrypted>

38 <https://www.bbc.co.uk/news/articles/cvgn1lz3v4no>

39 <https://www.washingtonpost.com/technology/2025/03/14/apple-encryption-backdoor-uk-order/>

40 <https://www.ft.com/content/330291f9-e765-47c1-8a29-f22a95674de9>

41 <https://www.openrightsgroup.org/blog/the-case-for-encryption/>

42 <https://www.openrightsgroup.org/blog/queercryption-safety-in-numbers/>



Sara Alsherif, ORG's Migrant Digital Justice Programme Manager, hosting a community event on AI in the asylum system in Brighton

MIGRANT DIGITAL JUSTICE PROGRAMME

Since 2020, ORG has been working at the intersection of digital rights and migration. Working alongside migrant rights organisations, ORG seeks to build capacity and strengthen the digital rights expertise in the sector, while raising the concerns of migrants within traditional tech and digital rights spaces. As an organisation, we work to expose and challenge the digitisation of the UK government’s hostile environment policy in legislation and practice.

Strengthening our Network

As part of our aims to strengthen our network, we carried out a number of activities to empower migrant and racialised groups. At the start of the year, we devised a new video training workshop, delivered with Praxis, to empower migrants to tell their own stories rather than relying on sympathetic media. Attendees were women looking to share their lived experience of the immigration system in the UK, and each received free equipment and training in narrative framing and editing. Participants reported feeling more confident sharing their stories on their own terms and said the training relieved the stress around sharing their stories online.

In collaboration with Positive Action In Housing and Migrants in Culture, we also

created a ‘Know Your Digital Rights’ toolkit⁴³ for migrants, focusing on how to exercise their right to submit Subject Access Requests (SARs). The guide breaks down SARs into actionable steps, complete with case studies on different scenarios, a summary of key protections, and templates for letters and emails. Throughout, we prioritised accessibility, with font-choice and design led by a specialist in dyslexia, translations into four languages, and illustrations created by an artist with lived experience. We will be publishing the Cantonese, Kurdish, Arabic, and Somali versions in the coming year.

Finally, thanks to our corporate supporters, we were able to provide migrants with free VPNs to help them keep their data secure.

Campaigning against eVisas

The UK’s shambolic eVisa scheme has left migrants unable to prove their right to work and live in the UK, with devastating consequences: people have lost job offers, missed out on university places and have even been made homeless.

From the start of 2025, we have continued to campaign against the scheduled rollout. Having secured an initial delay to the full roll-out to April 2025, we pushed for an

⁴³ <https://www.openrightsgroup.org/publications/know-your-digital-rights-a-guide-to-subject-access-requests/>

additional delay to June in order to give the Home Office time to resolve ongoing issues. Despite multiple meetings with the Home Office, who regularly fielded team members who lacked the technological expertise we had asked for, we were unable to establish exactly how the eVisa works, if not through live look-up.

We spoke about this at an event in parliament, chaired by John McDonnell MP. We also worked closely with other MPs, including Dawn Butler MP, to raise concerns about the scheme, table questions to the Home Office and push for offline alternatives, such as paper or downloaded digital documents. We mobilised our base to help us with this, and 130 of our supporters have written to their MP asking for this alternative.

The Immigration White paper declared the eVisa scheme a success and said that eVisas would be used to support immigration raids. 139 of our supporters wrote to their MPs condemning this decision and asking for this not to happen.

Throughout the year, we collaborated with Migrant Voice, the University of Warwick and the University of Leicester to explore the harms of digital ID on migrants. In December, we launched our joint research⁴⁴ revealed the emotional and practical toll the scheme takes and forewarned what could happen if digital ID is rolled out to everyone. Participants reported high levels of stress, fear and exhaustion as they attempted to navigate unclear guidance, shifting deadlines and frequent technical problems. There was also evidence that migrants were being asked to prove their right to be in the UK by members of the public who have no right to make such a demand, highlighting the risks of mission creep and racial profiling. We held an event to share our findings, which was attended by other NGOs and covered by industry press, including Computer Weekly⁴⁵ and Biometric Update.⁴⁶

⁴⁴ <https://www.openrightsgroup.org/publications/exclusion-by-design-digital-identification-and-the-hostile-environment-for-migrants/>

⁴⁵ <https://www.computerweekly.com/news/366636198/Error-prone-eVisa-system-a-precursor-of-digital-ID>

⁴⁶ <https://www.biometricupdate.com/202512/report-claims-uk-evisa-system-uses-migrants-as-digital-id-testing-ground>

Border Security, Asylum and Immigration Bill

We developed a briefing on the Border Security, Asylum and Immigration Bill, which we shared with MPs. We also submitted draft amendments, which were tabled by the Lib Dems. The amendments highlighted the lack of authorisation and oversight needed for law enforcement to access to migrant data.

Big Tech and Migration

We conducted research into how Meta’s surveillance advertising model enables vulnerable people to be targeted with disinformation, fraudulent ads and divisive content. Looking through a migration lens, we also found that Meta monetises the migrant crisis from both sides: firstly, through ads placed by criminals promoting false driving licenses and passports, and by the Home Office promoting fear-based campaigns to deter people from crossing the Channel in small boats. This has wider ramifications for democracy too, with this micro-personalisation lending itself to voter suppression, the targeting of minorities with electoral disinformation and political manipulation. This research formed part of our call for a clear and explicit opt-in for targeted advertising on Meta platforms.

Digital Sanctuary

As part of a new campaign, we have begun to work on the concept of “Digital Sanctuary”. Thanks to input from MRGs and CSOs in the UK, as well as organisations attending the EDRi and Global Gathering conferences, at which we hosted panels on the subject, we are putting together a comprehensive package of policies that would protect migrants in the digital world, pre-empting the legislative erosion of rights to privacy and freedom of expression.

PRE-CRIME

Through this programme, we oppose the use of digital “innovations” in law enforcement and counter-terrorism that do little to address the underlying social problems. Working in collaboration with a network of racial, social and criminal justice organisations, we investigate and challenge the ways in which data are leveraged as indicators of future crimes.

Challenging Predictive Policing

At the start of the year, we developed a number of amendments to push against predictive policing in the Crime and Policing bill, tabled by Sian Berry MP. We also raised awareness of last minute changes to the Policing Bill that would give the police the powers to extract data through a seized device to any online accounts that have been accessed by that device. Following on from this, we contributed to the Race and Community APPG where the conversation was specifically about crime predicting tech.

We launched an action calling for supporters to ask their councils to ban live facial recognition. Building on the success of this tactic in Islington, Newham and Haringey, where councils have already put forward motions to stop live facial recognition, we want to build more opposition at the lower levels of government. While councils have limited control over police use of live facial recognition, a groundswell of opposition at a council-level would demonstrate the community’s position and put pressure on the Met and other police forces.

#SafetyNotSurveillance Coalition

Established in 2024, our #SafetyNotSurveillance coalition is now well-established and received specific funding from the Joseph Rowntree Reform Trust in April 2025. Comprising over 30 members, including community groups and national NGOs, the coalition calls for an outright ban on predictive policing systems. These are systems which use AI, data and algorithms to identify, profile and target individuals, as well as to prioritise geographic areas to deploy resources.

The coalition collaborated on amendments for the Crime and Policing Bill, and together we engaged a number of local councils and MPs.

We also worked together on a response to the Home Office consultation on live facial recognition technology, which was an excellent example of the coalition’s role in platforming marginalised voices, as individual responses would have been too burdensome for most community groups.

In November, the Safety Not Surveillance coalition carried out a publicity stunt outside the Police Chief’s conference, led by ORG and Amnesty UK. The conference was attended by military vendors looking to sell technology and tools to UK police forces. Staff hung banners and held placards while others conducted vox pops with attendees about predictive policing. We hired a van to drive around London playing educational videos about predictive policing, as well as creating a range of content about this stunt for our social networks to encourage people to sign up to our campaign.

Footage from the stunt was posted on social media⁴⁷ and garnered thousands of views and over 300 engagements. The stunt was covered by journalists from Arte TV, who interviewed SnS coalition members, and ORG’s Sara Chitseko, Pre-Crime programme manager, spoke about the stunt and AI generally on the Black Policy Institute⁴⁸ podcast.

Investigating the Digital Harm of the Prevent Duty

Since 2023, we have played an important role in the sector by exploring the intersection of data protection and surveillance. This has been key when working to analyse and critique Prevent, a counter-terrorism programme that is ostensibly promoted as a safeguarding measure for individuals who are susceptible to extremism.

Our research over the years has found that despite not being charged with an offence, Prevent referees’ rights are infringed. Referees, who are disproportionately Muslim, neurodiverse and/or children, can be denied college places, stopped at airports when going on holiday, and refused rental opportunities. This incursion is compounded when the Prevent referee is managed under a police-

47 <https://www.instagram.com/reel/DRNRT63jxmA/?igsh=YWVpenB3dzZjNDE2>

48 <https://theblackpolicyinstitute.org/media>

led partnership (PLP) process, rather than the multi-agency ‘Channel’ process. These cases are normally assigned to police due to certain “risk” factors, such as a referee’s involvement in Palestinian solidarity campaigns. Together with Prevent Watch, academic Professor Charlotte Heath-Kelly and DPG Law, ORG has devised a research project into police-led partnerships under Prevent. This project received funding at the end of the year and will run until 2029, exploring grounds for litigation.

Towards the end of the year, ORG wrote to Ofcom and to Meta, Alphabet, X and ByteDance, asking for clarification over how they will protect the right to freedom of expression online in light of the proscription of Palestine Action as a terrorist organisation. We raised concerns that legal duties under the Online Safety Act, combined with the UK’s vague definition of terrorism, could lead to content being wrongly identified as illegal and removed. Our position is that platforms are incentivised to censor content to avoid the risk of fines, and discouraged from protecting freedom of expression and public debate.

Digital ID

Throughout the year, ORG warned that the UK risked creating a pre-crime state by introducing mandatory ID cards for everyone who works in the UK. We argued that once a national digital ID system is in place, mission creep is inevitable. Putting the infrastructure in place will increasingly force people to use their digital ID in everyday life, opening the door to unprecedented tracking of our interactions with the state. We organised a joint briefing with 12 other NGOs, outlining our concerns about the government’s proposals. These include the potential for mission creep, privacy and security risks, and discrimination and exclusion.

We were quoted extensively on the subject by media, including the BBC,⁴⁹ The Express,⁵⁰ and Computer Weekly,⁵¹ as well as being interviewed on Talk Radio, BBC radio and BBC radio Wales.

49 <https://www.bbc.co.uk/news/articles/c4g54g6vgpdo>

50 <https://www.express.co.uk/news/uk/2113836/starmer-digital-id-cards-risk-hackers-cybersecurity>

51 <https://www.computerweekly.com/news/366631981/Keir-Starmer-launches-digital-ID-scheme-but-does-it-stand-a-chance>

SUPPORT OUR WORK

Open Rights Group was founded by members of the public who decided the UK needed an organisation that would fight for their digital rights. Ever since, this grassroots support has been fundamental to who we are and how we win.

Today, we are fighting abuses by some of the most powerful opponents the world has ever seen – big tech companies who have our government in their pockets. And as you can see from the extent of our work over the past year alone, this is not an easy fight to win.

But our power comes from our members: people on the ground who want to join the fight. You tell us about the digital harms you are experiencing. You help us to lobby MPs and policymakers. You make a difference however you show up – signing petitions, emailing MPs, coming to events and joining local groups.

ORG doesn’t accept money from the government or big tech. Please join us to fight for digital rights. Together we can make a difference.

■ [Sign up to our newsletter](#)

■ [Join as a member](#)

■ [Volunteer with us](#)

■ [Fund our work](#)

Hannah Little



ACCOUNTANT'S REPORT

For The Year Ended 31 December 2025

You consider that the company is exempt from audit for the year ended 31 December 2025. You have acknowledged, on the Statement of Financial Position, your responsibilities for complying with the requirements of the Companies Act 2006 with respect to accounting records and the preparation of the accounts. These responsibilities include preparing accounts that give a true and fair view of the state of affairs of the company at the end of the financial year and its profit or loss for the financial year.

In accordance with your instructions, we have prepared the accounts which comprise the Income Statement, Statement of Financial Position and the related notes from the accounting records of the company and on the basis of information and explanations you have given to us. As advised by the Company Officers, based on previous communications with HMRC, the accounts have been prepared on the basis that the company has exempt status for corporation tax purposes.

The accounting records and explanations provided appear to be reasonable, however we have not carried out an audit or any other review, and consequently we do not express any opinion on these accounts.

Urban Ledgers Ltd

08/06/2026

Urban Ledgers Limited
124 City Road
London
EC1V 2NX

INCOME STATEMENT

For The Year Ended 31 December 2025

	NOTES	2025 £	2024 £
TURNOVER		743,802	846,815
GROSS SURPLUS		743,802	846,815
Administrative expenses		(739,560)	(844,393)
OPERATING SURPLUS		4,242	2,422
Other interest receivable and similar income		1,219	305
SURPLUS FOR THE FINANCIAL YEAR		5,461	2,727

The notes on pages 26 to 28 form part of these financial statements.

STATEMENT OF FINANCIAL POSITION

As At 31 December 2025

	NOTES	2025 £	2024 £
FIXED ASSETS			
Intangible Assets	4	17,935	-
Tangible Assets	5	1,937	4,012
		19,872	4,012
CURRENT ASSETS			
Debtors		16,392	16,302
Cash at bank and in hand	5	506,135	620,929
		522,527	637,231
CREDITORS: AMOUNTS FALLING DUE WITHIN ONE YEAR	7	131,377	141,776
NET CURRENT ASSETS (LIABILITIES)		131,377	141,776
TOTAL ASSETS LESS CURRENT LIABILITIES		151,249	145,788
NET ASSETS		151,249	145,788
Income Statement		151,249	145,788
MEMBERS' FUNDS		151,249	145,788

The notes on pages 26 to 28 form part of these financial statements.

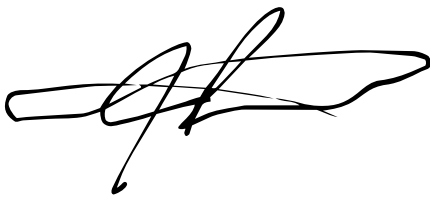
For the year ending 31 December 2025 the company was entitled to exemption from audit under section 477 of the Companies Act 2006 relating to small companies.

The members have not required the company to obtain an audit in accordance with section 476 of the Companies Act 2006.

The directors acknowledge their responsibilities for complying with the requirements of the Act with respect to accounting records and the preparation of accounts.

These accounts have been prepared in accordance with the provisions applicable to companies subject to the small companies regime.

On behalf of the board



Hannah Little
Director
08/06/2026

NOTES TO THE FINANCIAL STATEMENTS

For The Year Ended 31 December 2025

1. General Information

Open Rights is a private company, limited by guarantee, incorporated in England & Wales, registered number 5581537. The registered office is Space4 113-115 Fonthill Road, London, N4 3HH.

The prior year comparative figures are for a 14-month period from 1 November 2023 to 31 December 2024. The current year figures are for a 12-month period from 1 January 2025 to 31 December 2025.

2. Accounting Policies

2.1. Basis of Preparation of Financial Statements

The financial statements have been prepared under the historical cost convention and in accordance with Financial Reporting Standard 102 section 1A Small Entities "The Financial Reporting Standard applicable in the UK and Republic of Ireland" and the Companies Act 2006.

2.2. Turnover Income recognition

The company's income represents amounts receivable in furtherance of its principal objective of promoting awareness and understanding of digital rights matters. All income is applied solely towards the achievement of the company's objects and any surplus is retained within the accumulated fund for use in future activities and projects. As a company limited by guarantee, without share capital, the surplus cannot be distributed to shareholders.

Income is recognised when the company is entitled to the income, it is probable that the economic benefits will flow to the company and the amount can be measured reliably.

Supporter donations and Membership income are recognised in the period in which they are received. Grants and similar income are recognised in the Income Statement in an appropriate manner that matches them with the expenditure towards which they are intended to contribute.

Grants for immediate financial support or to cover costs already incurred are recognised immediately in the Income Statement. Grants towards general activities of the entity over a specific period are recognised in the Income Statement over that period.

Grants towards fixed assets are recognised over the expected useful lives of the related assets and are treated as deferred income and released to the Income Statement over the useful life of the asset concerned.

2.3. Intangible Fixed Assets and Amortisation - Other Intangible

Other intangible assets are software development. It is amortised to the Income Statement over its estimated economic life of 5 years.

2.4. Tangible Fixed Assets and Depreciation

Tangible fixed assets are measured at cost less accumulated depreciation and any accumulated impairment losses. Depreciation is provided at rates calculated to write off the cost of the fixed assets, less their estimated residual value, over their expected useful lives on the following bases:

Cycle Scheme 33% Straight Line

Office Equipment 33% Straight Line

2.5. Financial Instruments

The company only have financial assets and financial liabilities of a kind that qualify as basic financial instruments. Basic financial instruments are recognised at transaction value and subsequently measured at their settlement value.

2.6. Supporter Donations

Regular supporter donations are treated on a cash basis, i.e. are treated as pertaining to the month in which they are received.

3. Average Number of Employees

Average number of employees, including directors, during the year was: 13 (2024: 11)

4. Intangible Assets

	SOFTWARE DEVELOPMENT £
COST	
As at 1 January 2025	-
Additions	20,304
As at 31 December 2025	20,304
AMORTISATION	
As at 1 January 2025	-
Provided during the period	2,369
As at 31 December 2025	2,369
NET BOOK VALUE	
As at 31 December 2025	17,935
As at 1 January 2025	-

5. Tangible Assets

	CYCLE SCHEME £	OFFICE EQUIPMENT £	TOTAL £
COST			
As at 1 January 2025	280	28,466	28,746
Additions	-	638	638
As at 31 December 2025	280	29,104	29,384
DEPRECIATION			
As at 1 January 2025	87	24,647	24,734
Provided during the period	94	2,619	2,713
As at 31 December 2025	181	27,266	27,447
NET BOOK VALUE			
As at 31 December 2025	99	1,838	1,937
As at 1 January 2025	193	3,819	4,012

6. Debtors

	2025 £	2024 £
DUE WITHIN ONE YEAR		
Prepayments and accrued income	16,142	16,302
Other debtors	250	-
As at 31 December 2025	16,392	16,302

7. Creditors: Amounts Falling Due Within One Year

	2025 £	2024 £
Trade creditors	13,527	10,192
Other taxes and social security	17,723	14,523
Accruals and deferred income	359,900	470,740
	391,150	495,455

8. Company limited by guarantee

The company is limited by guarantee and has no share capital. Every member of the company undertakes to contribute to the assets of the company, in the event of its winding up, such amount as may be required, not exceeding £1.

9. 2025 Grant Income Analysis

	2025 £	2024 £
Luminate Big Tech and Data Protection	121,100	27,723
ISOC Encryption 2024	Nil	6,502
Digital Freedom Fund	Nil	27,486
Duck Duck Go	22,684	19,992
Joseph Rowntree Reform Trust Ltd	24,617	19,275
Oak Foundation	137,965	144,763
Open Society Foundation	117,596	179,771
Paul Hamlyn Foundation	56,112	70,923
ESRC Digital Good	992	2,976
Reset	Nil	86,752
EDRI Platform	3,754	Nil
John Ellerman 2024	39,996	Nil
TOTAL	524,816	586,163

DETAILED INCOME STATEMENT

For The Year Ended 31 December 2025

	2025 £		2024 £	
TURNOVER				
Business membership		11,644		8,557
Grants		524,816		586,163
Supporter donations		156,250		188,899
Internal fund income		44,544		60,546
Cycle to work scheme		-		280
Gifts and donations income		6,030		2,341
Surplus on asset sales		-		29
Miscellaneous income		518		-
		743,802		846,815
GROSS SURPLUS		743,802		846,815
ADMINISTRATIVE EXPENSES				
Salaries	578,173		605,182	
Contractors and specialists	12,639		7,491	
Staff training	185		4,253	
Staff recruitment	-		7,002	
Travel and subsistence	10,156		10,554	
Rent and rates	3,051		4,473	
Insurance	1,677		1,913	
Postage and printing	899		1,103	
Website costs	120		183	
Accounting and other professional fees	6,454		9,784	
ORGCon and public event costs	113		130	
General campaigning	56,881		91,689	
Strategy and planning	10,411		25,975	
Strategic litigation	16,080		17,317	
Service providers	14,989		30,955	
Associations and memberships	8,395		7,563	
Donation processing charges	3,488		5,929	
Bank charges	549		821	
Office supplies and telephony	4,296		4,459	
Depreciation	2,712		5,852	
Amortisation	2,369		-	
Foreign exchange losses/(gains)	3,358		(6)	
Other expenditure	2,565		1,771	
		(739,560)		(844,393)
OPERATING SURPLUS		4,242		2,422
OTHER INTEREST RECEIVABLE AND SIMILAR INCOME		131,377		141,776
Bank interest receivable	1,219		305	
		1,219		305
SURPLUS FOR THE FINANCIAL YEAR		5,461		2,727



