

# The UK Safety Tech Sector: 2024 Analysis

DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY  
UK ONLINE SAFETY TECHNOLOGY SECTORAL ANALYSIS

# Contents

<b>1. Introduction and Background</b>	<b>8</b>	<b>5. Estimated Revenue &amp; Employment</b>	<b>22</b>
1.1 Introduction	8	5.1 Introduction	22
1.2 Team & Acknowledgements	10		
1.3 Scope	10	<b>6. Investment in Safety Tech Providers</b>	<b>28</b>
1.4 Methodology	11		
		<b>7. Supporting Growth in the Sector</b>	<b>32</b>
<b>2. Defining the Safety Tech sector</b>	<b>12</b>		
2.1 Background	12	<b>8. Appendices</b>	<b>44</b>
		Appendix A: Methodology	45
<b>3. Market Profile</b>	<b>14</b>	Appendix B: Taxonomy Update	47
3.1 Number of Safety Tech Providers	14		
3.2 Products and Services	15		
<b>4. Location</b>	<b>20</b>		

## Ministerial Foreword

The Online Safety Act, which received Royal Assent in 2023, took significant steps to encourage safer online spaces while protecting freedom of expression. Regulation alone, however, is not enough to achieve our online safety objectives. We must also recognise the important role of technology and, in particular, the role the UK's world-leading safety tech sector plays in protecting users online.

Our sectoral analysis has been tracking the UK's safety tech sector annually since the publication of the first Safer Technology, Safer Users report in 2020. This set out the UK's role in developing solutions that are being used worldwide to protect users and to detect and remove illegal content.

Since that time, the sector has experienced an impressive period of continuous growth driven by UK innovators committed to making online environments safer. Our latest research reveals that there are now 143 safety tech businesses operating in the UK, that revenue has increased 37% year-on-year to £623mn, and that expertise spans age assurance, brand and platform safety, digital forensics, content filtering, and combating issues such as fraud and disinformation. This range of technologies solidifies the UK's position at the forefront of tackling online harms and equips our digital economy and tech platforms with tools to ensure user safety.

As technology evolves at an unprecedented pace, it is crucial that we remain agile in protecting UK citizens appropriately. The UK safety tech sector has risen to this challenge, establishing itself as one of the fastest-growing tech sectors in the country. With a workforce that now exceeds 3,900 employees nationwide, the sector's expansion underscores its significance and impact.

Interest from external investors has kept pace to enable this continued growth. While macro factors meant 2023 saw a significant slowdown in tech investment and declining deal sizes globally, the volume of investment into UK safety tech businesses remained steady while the number of investments increased from 16 to 18. This demonstrates the confidence in the UK's safety tech sector and its potential for continued growth and innovation.

The government is committed to taking forward a broad range of initiatives to support innovation and the safety tech sector. We will seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models, which will help to strengthen the UK's role as a global leader in safe and trustworthy AI. We will also continue to work closely with international partners to promote coordinated action, while identifying opportunities to collaborate with likeminded international partners.

The safety tech sector is a key part of ensuring that the UK remains both the safest place to be online, and a leading location for developing innovative solutions to keep users safe online. We will continue to support the sector, and by working together, we will build a safer digital world for all.

### **BARONESS JONES OF WHITCHURCH**

Parliamentary Under-Secretary of State for the Future Digital Economy and Online Safety



## KEY FINDINGS

This section sets out the key findings from this year's Safety Tech Sectoral Analysis.

### Evidence of Continuing Sectoral Growth

- The UK's safety tech sector consists of an estimated 143 dedicated providers, offering a wide range of products and services across the safety tech taxonomy.
- The sector has demonstrated rapid revenue growth, with an estimated total revenue of £623m in 2023, marking a 37% increase from the previous year and nearly tripling in size since the baseline study in 2020.
- The sector is on track to reach the baseline target of £1bn in annual revenues by 2025/26, with a compound annual growth rate of 29% between 2020 and 2024.
- The sector currently employs approximately 3,900 people in the UK, an 18% increase from the previous year, with employment well-distributed across UK regions.
- The UK safety tech sector is globally significant, with the UK accounting for an estimated one-in-four (23%) of the global safety tech workforce.
- The sector demonstrates strong potential for further growth and innovation, with 91 out of 143 UK safety tech providers currently exporting their products and services internationally.

### Robust Investments and Funding Despite Challenging Conditions

- Investment in the sector remains strong despite wider challenging conditions, with £42m raised across 18 deals in 2023, demonstrating sustained investor appetite for safety tech firms.
- The sector is attracting global international

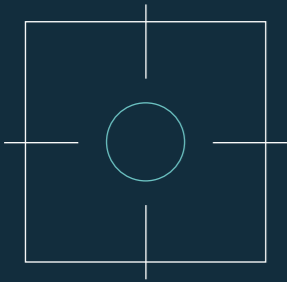
attention and investment as reflected in the International State of Safety Tech research. Further, the UK is seen as an attractive destination for safety tech inward investment.

### Emerging Trends in Business Models and Routes to Market

- The research suggests that growth areas within the sector include brand safety, fraud detection, and the use of open-source intelligence (OSINT) and social media intelligence (SOCMINT) in wider service provision.
- The emergence of 'Safety Tech as a Service' (STaaS) is a notable trend, with growing demand for outsourced safety tech solutions.
- The safety tech sector is maturing, with an increasing number of firms demonstrating growth and scale. The number of large and medium-sized firms has increased considerably since the previous year, with 25 large and medium firms now operating in the UK safety tech sector (compared to 16 last year).
- Collaboration and partnerships are driving growth in the sector, with over 600 partnerships mapped between safety tech providers and their clients, highlighting the increasing adoption of safety tech solutions across various industries.



# 1. Introduction



The Department for Science, Innovation and Technology (DSIT) has tracked the growth of the UK's safety tech sector since May 2020, through the annual 'Safety Tech Sectoral Analysis' research project.

This research provides an overview of the UK's capabilities in its online safety technology ('safety tech') sector, and has identified significant growth in recent years, driven by a range of highly innovative companies focused on tackling online harms through technical solutions.












This report marks the fifth annual review of the sector's performance and finds further evidence of a high-growth and high-potential sector. It also suggests that the sector is well-positioned to achieve the projected target set out within the 2020 baseline, of reaching £1bn in annual revenues by 2026/27.

## DEFINITION AND SCOPE:

In order to identify relevant companies within the sector, the following definition is used:

"Safety Tech providers develop technologies or solutions to facilitate safer online experiences, and protect users from harmful content, contact or conduct."

## THIS FOCUSES ON FIRMS THAT:

-  Often work closely with law enforcement, to help **trace, locate and facilitate the removal of illegal content** online
-  Work with social media, gaming, and content providers to **identify criminal, harmful or toxic behaviour** on their platforms
-  **Monitor, detect and share online harm threats** with industry and law enforcement in real-time
-  Develop trusted online platforms that are **age-appropriate** and provide parental reassurance for when children are online
-  Use technology to **identify, prevent, and mitigate real-world harmful incidents** from occurring, or respond to events
-  Detect, disrupt and protect users from **fraudulent advertisements**
-  **Verify and assure** the age of users
-  Actively identify and respond to instances of **online harm, bullying, harassment and abuse**
-  Help organisations to **filter, block and flag harmful or illegal content** at a network or device level
-  **Detect and disrupt false, misleading or harmful narratives** (mis- and disinformation)
-  Advise and support a community of moderators to **identify** and remove harmful content

Perspective Economics, with support from PUBLIC and Professor Mary Aiken (University of East London), has been commissioned by the Department for Science, Innovation & Technology (DSIT) to conduct an updated safety tech sectoral analysis exercise.

This report explores the number of businesses offering safety tech products and services and provides an updated market estimate of the size of the sector in the UK, measured through revenue, employment, and external investment. It remains consistent with the updated taxonomy set out within the 2023 Safety Tech Sectoral Analysis, to ensure there is a consistent longitudinal evidence base to help track the long-term growth of the UK safety tech sector.

## 1.2 TEAM AND ACKNOWLEDGEMENTS

DSIT and Perspective Economics would like to acknowledge the consultees, nationally and internationally, who contributed to the development of this report through participation in consultations and survey activity with the research team. In total, the research engaged with more than thirty industry and policy representatives.

The safety tech sector has consistently demonstrated significant growth each year in the UK. Further, it continues to support government, civil society and industry in tackling and mitigating the impact of harmful and illegal activity online and developing new solutions to novel and emergent harms.

## 1.3 SCOPE

This research seeks to identify providers of safety tech products or services, with a clear presence in the UK market (UK registered), and that are active and undertake commercial activity. For research purposes, the following are considered within this report; however, we recognise the broader contribution of many organisations involved within the wider online safety ecosystem.

### RESEARCH SCOPE

For the purposes of this research, safety tech providers are defined as organisations which:

- ✓ Have a clear presence in the UK market (registered and active status)
- ✓ Demonstrate an active provision of commercial activity related to online safety technology (e.g. through the presence of a website / social media)
- ✓ Provide safety tech products or services to the market (i.e. sell or enable the selling of these solutions to other customers)
- ✓ Have identifiable revenue or employment within the UK

Section 2 of this report sets out the type of organisations within scope and sets out the products and services typically offered by market providers.

## 1.4 METHODOLOGY

The methodology for this research is consistent with that set out in Appendix B of the 'Safer Technology, Safer Users' report (2023).

The research team uses the existing safety tech sector taxonomy and has applied additional markers to identify the range of products and services provided by safety tech companies. The research has identified 143 'dedicated' companies using web data, financial data, procurement data, and through direct consultation with industry. These companies have been reviewed by the research team and confirmed as relevant to the safety tech sector.

All firms have been reviewed and enriched using:

### COMPANY ACCOUNTS

The research team has identified relevant financial metrics for each provider through the most recent UK financial accounts.

### WEB DATA

The research team has reviewed company websites to identify key product and service offerings, locations and markets served, customers (where mentioned), and relevant staff and team sizes (relating to safety technology).

## SURVEY AND CONSULTATION ACTIVITY

All providers were invited by DSIT and Perspective Economics to take part in a short online survey in February 2024. This explored company performance and growth expectations. It also asked providers about innovation and tackling harms in areas such as generative AI and the metaverse.

### WIDER DATASETS

Perspective Economics has established data partnerships with proprietary data providers to support the enrichment of data used for this study. This includes Beauhurst (a platform that tracks external fundraising and high-growth companies across the UK) and Tussell (a procurement database, which tracks contracts awarded by the public sector).

## 2. Defining the Safety Tech sector



### 2.1 BACKGROUND

*Safety tech providers develop technologies or solutions to facilitate safer online experiences, and to protect users from harmful content, contact or conduct.*

This definition was established in the baseline Safety Tech Sectoral Analysis (2020) report and expanded through a market taxonomy that provided scope to identify a range of products and services used to help make users safer online.

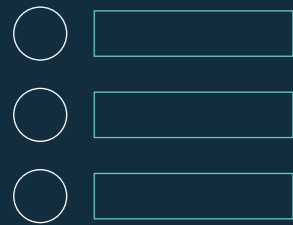
The definition above distinguishes the safety tech sector from adjacent sectors. For example, there may arguably be some overlap between safety tech and fields such as cyber security, FinTech, and RegTech; however, we seek to identify firms that are distinct in terms of focus on online safety, compared to areas such as data security.

In 2023, we updated the 'safety tech taxonomy' to reflect the evolving breadth and depth of the sector, with minor changes to allow for time-series analysis. The taxonomy has been developed to illustrate the scope of the safety tech sector and has primarily been used to support DSIT mapping and tracking of safety tech firms. The research also recognises diverse use cases and technologies within the safety tech sector and acknowledges that many firms within the sector can provide products or services across the different levels of the taxonomy.

It is also recognised that several of the larger tech companies are actively involved in the production or development of safety tech solutions (e.g., Microsoft's PhotoDNA, and AWS' Rekognition Image Moderation API). However, as with previous iterations, these providers are not measured within this sectoral analysis, which is focused on dedicated third-party safety tech providers. The UK also has a particularly active community of charitable and representative organisations involved in tackling issues relating to online safety, which are also excluded from this sectoral analysis.

The following sections set out the market profile, number of providers, location, commercial revenue and employment activity, and investment in the UK safety tech sector.

## 3. Market Profile



### 3.1 NUMBER OF SAFETY TECH PROVIDERS

Using the safety tech definition and taxonomy, we have identified 143 organisations dedicated to providing relevant safety tech products and services which are registered within the UK. However, we recognise that there are likely several further providers within the marketplace that have the relevant skills and expertise to become more involved with safety tech in future years.

These could include companies currently using AI or designing cyber security solutions focused on threat intelligence, or AdTech firms that focus on responsible advertising and brand safety, technologies that could arguably be deployed within the context of keeping users safer online for social purposes.

This is a trend that is likely to become more apparent, with an increased number of firms utilising Trust and Safety terminologies being identified during initial scoping exercises.

### 3.2 PRODUCTS AND SERVICES

For the 143 organisations identified for commercial analysis, we have identified company descriptions of what they offer by means of web data and direct consultation. The nature of this sector means that some organisations provide diverse products and services - for example, content moderation, sentiment analysis, and advisory services.

We have identified the best fit of each of the commercial organisations against the taxonomy categories to illustrate the overall sector composition. We have also applied multiple markers to each firm to enable analysis of firm products and services across multiple categories. This is set out within the final column in the table on page 16.



TABLE 1: TAXONOMY CLASSIFICATIONS OF THE UK SAFETY TECH SECTOR

TAXONOMY CLASSIFICATION	SHORT DEFINITION	NUMBER OF FIRMS (BEST FIT)	NUMBER OF FIRMS (WITH SOME OFFERING)
<b>System-wide governance</b>	Automated identification and removal of illegal content: use of technology to identify and enable the removal of illegal child sexual exploitation and abuse (CSEA) material, and terrorist content including imagery and video.	16 (11%)	21 (15%)
<b>Platform-level</b>	This includes organisations that support content moderation through identifying and flagging potentially illegal content or conduct, such as grooming, hate crime, harassment or suicide ideation or harmful content or conduct which breaches site T&Cs, such as cyberbullying, extremism or advocacy of self-harm. They also support identification and response to fraudulent activity or behaviour. Further, they may assist in reducing moderators' own exposure to harmful content.	34 (24%)	73 (51%)
<b>Age orientated online safety</b>	Enabling age-appropriate online experiences through use of age assurance and age verification services to limit childrens' exposure to harmful content, or development of child-safe content.	20 (14%)	66 (46%)

TAXONOMY CLASSIFICATION	SHORT DEFINITION	NUMBER OF FIRMS (BEST FIT)	NUMBER OF FIRMS (WITH SOME OFFERING)
<b>User Protection</b>	User, parental or device-based products that can be installed on devices to help protect the user from harm.	21 (15%)	42 (30%)
<b>Network Filtering</b>	Products or services that actively filter content, through blacklisting or blocking content perceived to be harmful. This can include solutions provided to schools, businesses, or homes to filter content for users.	14 (10%)	19 (13%)
<b>Information Environment</b>	Flagging of content with false, misleading and/or harmful narratives, through the provision of fact-checking and disruption of disinformation (e.g. with trusted sources).	20 (14%)	27 (19%)
<b>Online Safety Professional Services</b>	Advisory support with implementing technical solutions. Enabling the development of safer online communities and embedding safety-by-design.	18 (13%)	45 (31%)

Within the previous year, we have identified growth across all categories in the safety tech sector. However, we find that there has been particularly significant growth in providers in the platform level and information environment categories. This includes where some safety tech providers have developed new solutions to help protect brands from harmful contact or content. Within a market setting, the data suggests key areas of growth include:

#### BRAND SAFETY

Areas such as marketing, social media, and brand awareness are highly valuable markets for a wide range of sectors. For example, it may only take one social incident online, such as harmful content on a social media feed, or a concerted campaign against a certain brand or company to cause significant reputational or financial damage. As such, protecting brands from appearing alongside inappropriate or harmful content, and supporting companies that understand their digital footprint is a significant area of growth for safety tech firms.

#### FRAUD DETECTION

Aligned to this is the need to help both platforms and individuals identify and prevent various forms of online fraud. This can include fraudulent behaviour, counterfeit goods, or customers being exposed to bad actors (e.g., online marketplaces where transactions are not as expected). This means there is considerable market demand for **behavioural identification and response to bad actors (as-a-service)** to help detect and mitigate the impact of malicious users and their activities. This can also require the use of multiple safety technology domains such as identity and age verification, multi-model content moderation, and content provenance.

#### OPEN SOURCE INTELLIGENCE (OSINT) AND SOCIAL MEDIA INTELLIGENCE (SOCMINT)

The increasing spread of misinformation, deepfakes, and manipulated content online has created a growing market demand for AI-powered solutions that can verify the accuracy and authenticity of content. Safety tech businesses that develop tools leveraging machine learning, computer vision, and natural language processing to detect disinformation, manipulated media, and synthetic content may be well-positioned for market growth. Further, there is evidence of some safety tech firms engaging with areas such as LLM safety and scoring, reflecting the need for independent review of model safety, as well as safety of associated inputs and outputs.

#### GROWING DEMAND FOR STaaS

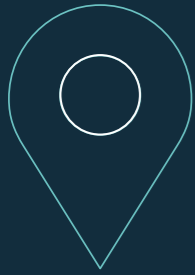
Many organisations recognise the importance of online safety but may lack the resources or expertise to develop and maintain in-house safety tech solutions. This has led to a growing demand for STaaS offerings, which provide organisations with access to safety technologies without the need for extensive internal development, or integrating a significant range of third-party APIs. Safety tech providers can offer a range of solutions, e.g. content moderation and age verification to fraud detection and threat intelligence, but delivered to platforms via a flexible and scalable model. This can often be more cost-effective for platforms, as they can scale the model depending on the extent of users and harm inherent to their platforms. It may also support platforms that deploy new innovations in safety tech (e.g., brand monitoring) and comply with changing regulations across different jurisdictions.

#### SAFETY TECH SERVICES MAY HELP TO STEM THE GAP IN TRUST AND SAFETY COVERAGE

Recent structural changes to trust and safety teams at major tech companies have potentially an opportunity for external online safety providers to help support with ongoing moderation and compliance. Throughout consultations, we find that some 'as a service' providers are well-positioned to fill this gap, by providing online safety support to platforms to ensure sustained compliance, and potentially also able to hire and recruit talent from former Trust and Safety teams. This means that outsourcing and a 'safety managed service' which captures areas such as regulatory compliance, age assurance, content moderation and brand protection may become a compelling solution for tech platforms – particularly as more businesses fall under the scope of global online safety legislation.

Within this study, we find that many providers active in the UK have grown their provision, and there has been a slightly slower rate of growth in new incorporations within the last two years. This may also be driven by several UK firms which have successfully identified a niche offering within the safety market, and been able to grow and secure investment relatively quickly. However, in the UK, we find evidence of some larger providers moving into the UK market.

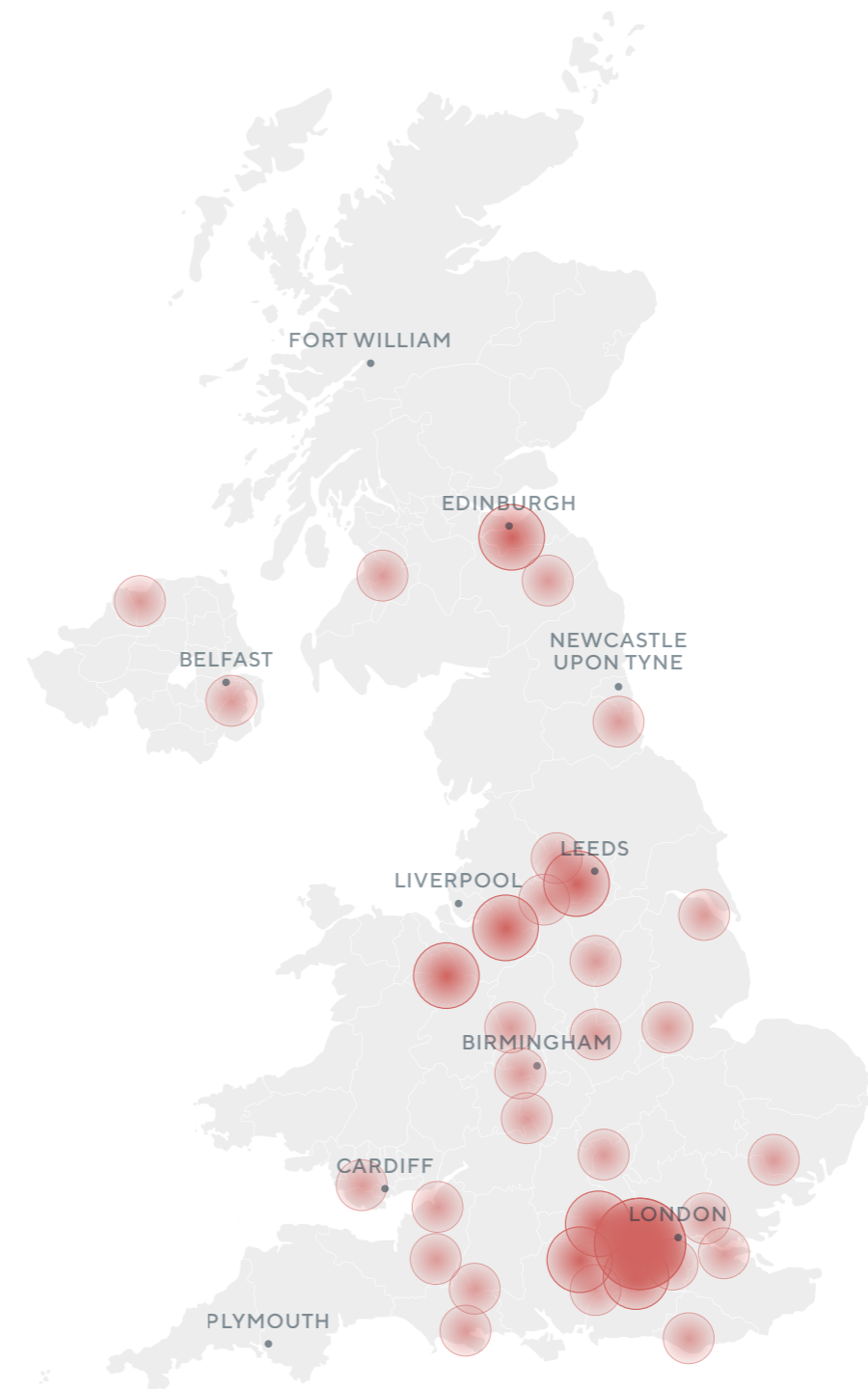
## 4. Location



This section sets out the location of safety tech providers, suggesting that nearly half (45%) have a registered or trading presence outside of London and the South East.

As set out in previous studies, there are also identifiable safety tech clusters in areas such as Leeds, Edinburgh and Cambridge.

FIGURE 2: LOCATION ANALYSIS OF THE UK SAFETY TECH SECTOR



Source: Perspective Economics, n = 143

## 5. Estimated Revenue & Employment



### 5.1 INTRODUCTION

This section outlines how the safety tech sector has grown in recent years, including estimates for annual revenue and employment.

Within the 2020 baseline report, the safety tech sector was noted as being a high-growth, but emerging and nascent market. Since then, the market has continued to grow in the UK at almost 30% per annum, despite wider challenging economic conditions.

Further, the growth of the UK's safety tech sector has acted as a catalyst to that of the global 'Trust and Safety' ecosystem. This is reflected in the 'International State of Safety Tech 2023' research by Paladin Capital, which highlights that "the United States and the United Kingdom together are leading the industry, collectively home to about three-quarters of safety tech companies", and that the "international safety tech market is experiencing rapid year-to-year growth. In the past three years alone, Safety Tech firms have raised \$4.8 billion. That is nearly triple the amount raised between 2011 – 2020."

We note that many organisations are at 'pre-revenue' or micro stage, and therefore do not provide full annual accounts. We therefore estimate total sectoral revenue through a mix of known company accounts, direct consultations, and company-level estimation as appropriate.

### KEY FINDINGS

- We estimate that total UK safety tech sector revenues for the last financial year (modal: FY ending 2022/2023) have reached £623m. This marks an increase of £167m (+37%) since last year's estimated revenue figure of £456m.
- This highlights the significant and sustained revenue growth within the safety tech sector. Since the first baseline report undertaken in 2020, the safety tech sector in the UK has almost tripled its annual revenue, with a compound annual growth rate of 29% between 2020-24.
- We anticipate that, in line with the baseline study projections, the sector is on track to reach the baseline target of £1bn turnover by 2025/26.
- We also estimate that across the UK safety tech sector, there are currently 3,900 Full-Time Equivalent (FTE) employees. This is an increase of 18% (+600 people) since last year's report.

The following subsections set out estimated company size, revenue, and employment.

### Estimated Company Size

Of the 143 organisations identified for commercial analysis, the majority are micro (<10 employees) or small firms (<50 employees) representing 47% and 36% of firms respectively.

However, when analysing size composition, we have found that more firms are demonstrating evidence of maturity year on year. In the previous report (2023), we identified one large firm (>250 employees), and fifteen (15) medium sized firms (firms with either over 50 employees, or turnover in excess of €10m).

In this year’s study (2024), this has increased considerably to four large firms, and 21 medium firms. A slight majority of firms (53%) are small, medium, or large overall – which suggests that the cohort of firms that may be ‘investment-ready’ or have potential to grow and scale is improving year on year, and this is reflected within the revenue growth.

TABLE 2: ESTIMATED COMPANY SIZE OF UK SAFETY TECH FIRMS (UK PRESENCE)

CATEGORY	DEFINITION	NUMBER OF FIRMS
Large	Employment > 250 And Turnover > €50m or Balance sheet total > €43m	4 (3%)
Medium	Employees >50 and <250 And Turnover > €10m and <€50m or Balance sheet total < €43m	21 (15%)
Small	Employees >10 and <50 And Turnover > €2m and < €10m or Balance sheet total < €43m	51 (36%)
Micro	Employment <10 And Turnover < €2m or Balance sheet total > €2m	67 (47%)
<b>Total</b>		<b>143</b>

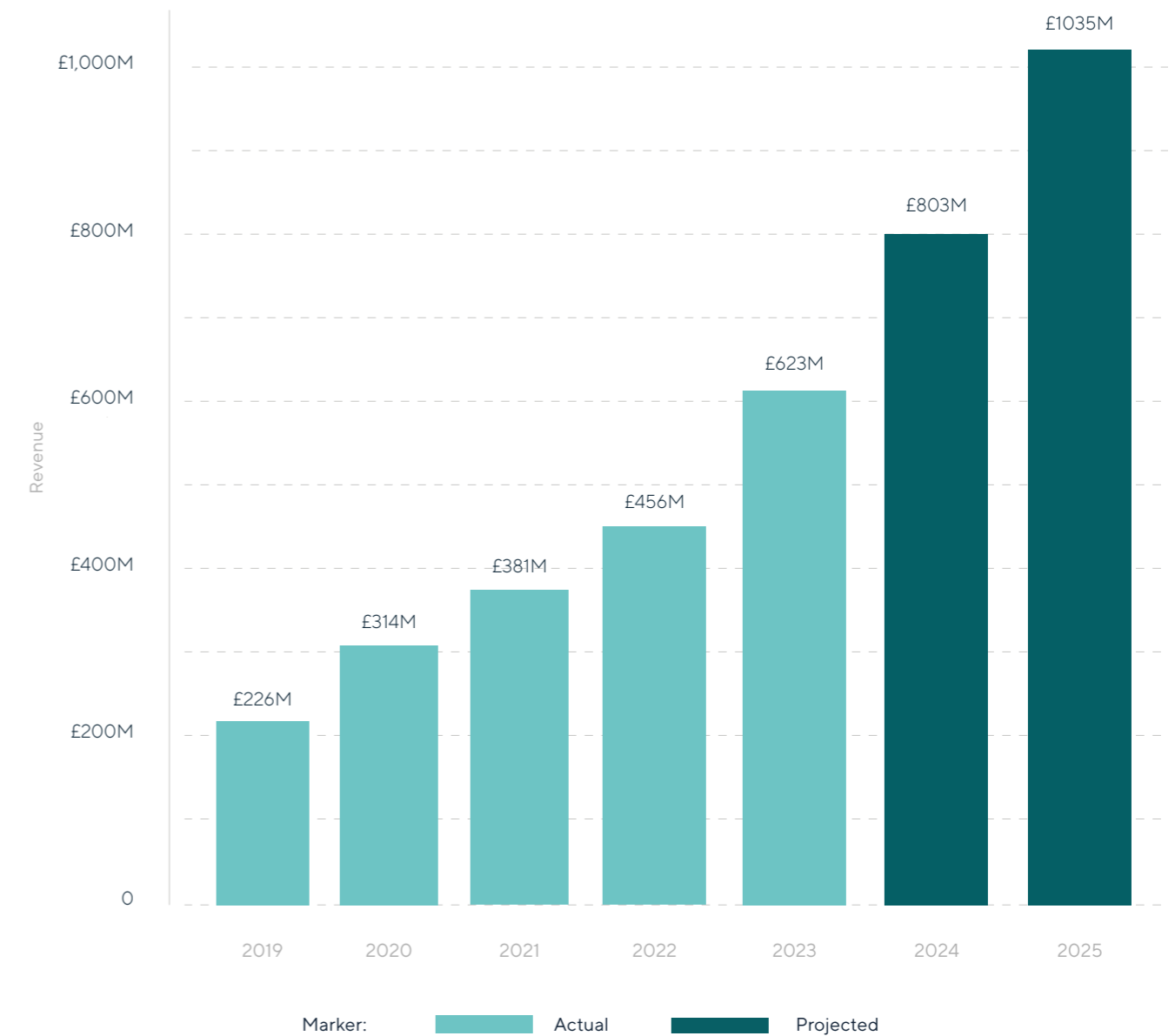
Source: Perspective Economics, n = 143 providers

### Estimated Revenue

We estimate that in total, the safety tech sector generated £623m in annual revenues in 2023. Figure 3 highlights how the sector has grown at a compound rate of 29% per annum since the baseline study.

This means that the sector has nearly tripled in size in the last five years, and appears on track to reach £1bn by 2025/26.

FIGURE 3: SAFETY TECH SECTORAL REVENUE (2019 - 2023, AND PROJECTED TO 2025)



Source: Perspective Economics sector revenue estimates (2020-23) and forecast

### Estimated Employment

We estimate that there are approximately 3,900 people working within dedicated safety tech firms based in the UK. This has been estimated through company accounts, web data and consultation data.

**This is an increase of 600 people since last year's report – marking employment growth of 18%.**

We find evidence that employment within the sector is well distributed across UK regions, with a slight majority (51%) in London, but wider hotspots including Yorkshire and the Humber (13%), North West (7%) and Northern Ireland (6%).

Regional employment is significant for the sector, with several of the largest safety tech providers in the UK including Resolver (formerly Crisp, a Kroll company) with over 250 and Yoti with over 200 staff operating outside of London and serving international markets.

The global 'International State of Safety Tech' research (2023) also suggests there are currently 16,600 employees working directly (excluding freelancers) for safety tech firms globally. This suggests that the UK is home to one-in-four (23%) of the global safety tech workforce.



## 6. Investment in Safety Tech Providers



This section sets out an overview of the investment landscape for the firms identified within this sectoral analysis, using the Beauhurst platform as an evidence source.

Beauhurst tracks announced and private investments, along with the performance of high-growth companies in the UK. It also monitors UK business participation within well-known business accelerator and incubator initiatives, and tracks where businesses have secured funding from public bodies such as Innovate UK.

### Investment Activity to Date

Within the last five years, the volume and value of external investment within safety tech companies has grown significantly.

In the first year we tracked (2015), the safety tech sector raised £6 million in external investment across ten deals.

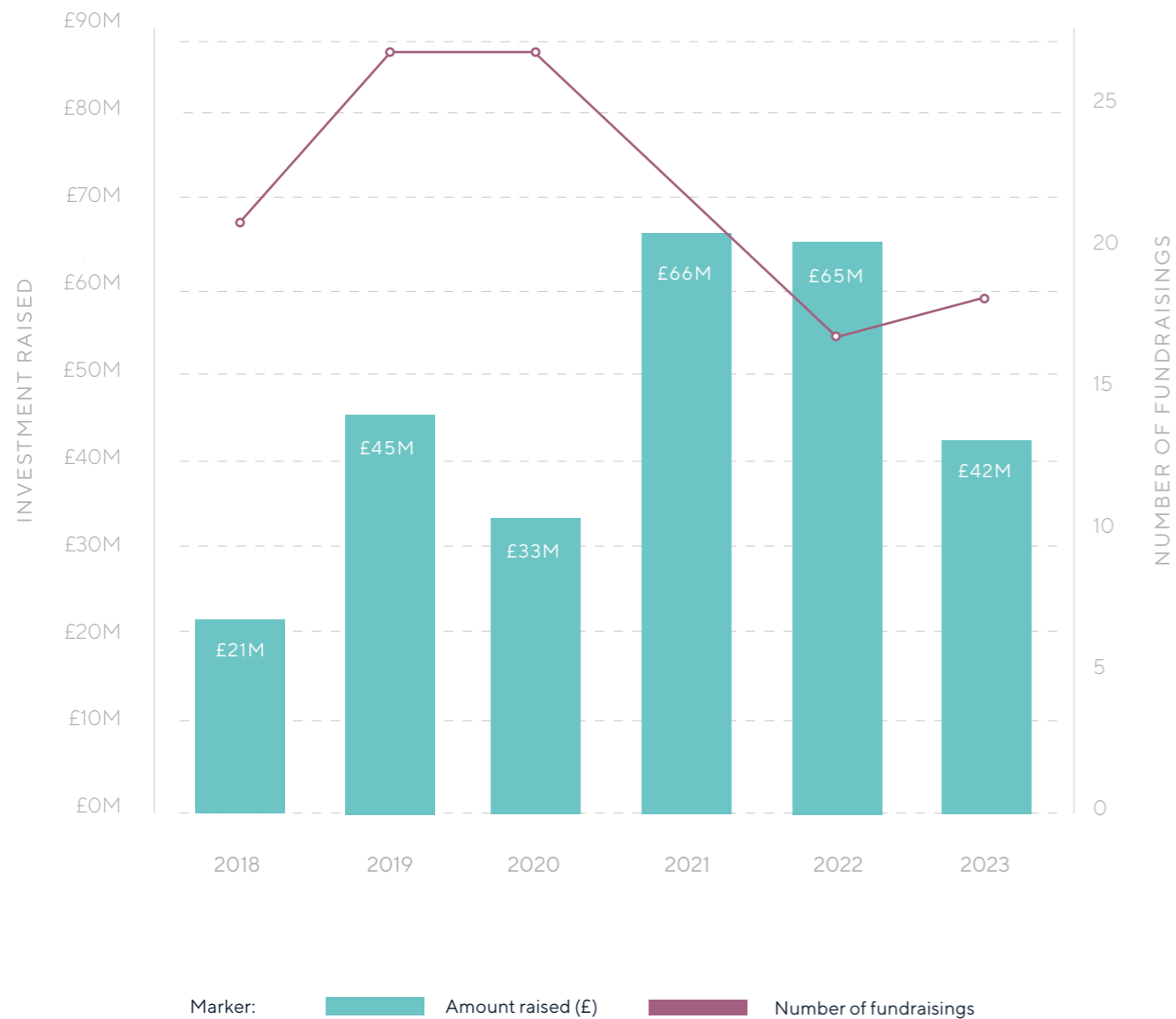
In last year's report (covering 2022), this increased tenfold to £65 million across sixteen deals, reflecting the increased scale and maturity of companies within the sector. Previous iterations of the safety tech sectoral analysis identified a number of high-growth success stories which reflect a growing understanding of the need for safety tech solutions.

However, the previous analysis also suggested that the investment landscape has become more challenging both for safety tech providers, and for tech platforms more generally. Consultees highlighted several sector specific factors influencing investment, including investor awareness of the sector, ability for firms to identify the right product to market fit, the policy landscape, and the infrastructure available to support the sector in raising investment (e.g., business support and accelerators relevant to safety tech firms).

As this data covers the previous full year (2023), it is retrospective in nature, and suggests that some of the challenges cited by safety tech providers have been borne out in the investment figures.

In 2023, total external investment has fallen from £65m to £42m (a reduction of 35%). However, the volume of deals has risen slightly (from 16 to 18), suggesting a maintained appetite among investors within safety tech firms, albeit with reduced deal values.

FIGURE 4: SAFETY TECH INVESTMENT RAISED (2018 - 2023)



Source: Perspective Economics

**Example Deals in 2023:**

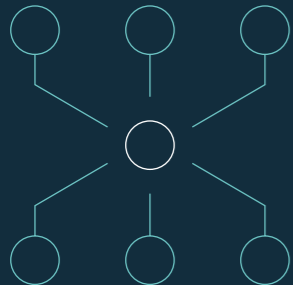
- Unitary** develops context-aware computer vision models to assess content such as video for potential harm. They specialise in content moderation, incorporating visual, audio and text signs into a single algorithm. This supports brands and platforms to reduce manual moderation and can review millions of posts per day. In 2023, Unitary raised over £19m across two deals. They raised \$15m in Series A funding in October 2023, led by Creandum with participation from Paladin Capital Group and Plural. This will be used to support launch across multiple languages, expand the team, and extend the capability of the platform<sup>1</sup>.
- Logically** combines AI with expert intelligence to tackle the impact of harmful online content at scale. It supports clients such as Meta and TikTok with fact-checking, and supports a range of public and private clients with detecting and responding to misinformation and disinformation. It also supports enhanced content moderation through signal enrichment. Since incorporation, it has raised over £36m, and secured £5m in equity fundraising in early 2024.
- VerifyMyAge** develops age verification software for e-commerce sites, using methods such as AI facial scanning, credit card or mobile phone data, credit checks or physical identification scans. It raised over £5m in 2023.
- Cyacomb** is a leading online safety company, that specialises in digital forensics (Cyacomb Forensics) to support law enforcement rigorously scan digital content at scale, finding and flagging harmful content while protecting database security and user privacy. It also has developed Cyacomb Safety, which includes detection and filtering technology that combats online child sexual abuse and terrorist content in end-to-end encrypted messaging platforms, on social media and in cloud platforms, whilst maintaining user privacy. Cyacomb has raised over £15m since launch and raised £4m in Q3 2023.
- AgeChecked** is a leading online age verification service provider. It provides age verifications services to companies to ensure their goods are sold appropriately. They raised over £2.6m in early 2024.
- Pasabi's Trust & Safety Platform** uses AI Behavioural Analytics and Network Science to tackle online fraudulent behaviour. They use cluster technology to identify a wide range of illegal and harmful activities including fake reviews, fraud rings, scams, fake accounts, counterfeit products and unauthorised sellers. They raised £2.4m in early 2023.
- GoBubble** develops a range of AI-powered software that moderates platforms, apps and social media feeds to filter hateful and abusive content. They raised £2m in early 2023.
- NetWatch Global** develops a range of AI-powered software that moderates platforms, apps and social media feeds to filter hateful and abusive content. They raised £725k in June 2023.
- SnapDragon Monitoring** provides bespoke brand protection packages to defend companies and brands from intellectual property infringement across the web. They have raised over £4m since launch and raised £600k in 2023.
- Whisp** instant, AI-powered fact-checking empowering people and organisations to verify claims, news articles, and other online information quickly and accurately. They raised over £500k in April 2023.

This deal data draws on the Beauhurst platform and wider public data

<sup>1</sup> <https://www.unitary.ai/articles/unitary-raises-15m-series-a-to-keep-digital-communities-safe-by-classifying-the-internets-information>



## 7. Supporting Growth in the Safety Tech Sector



### THE UK'S APPROACH TO ONLINE SAFETY:

The inaugural Safety Tech Sectoral Analysis in 2020 set out the extensive legislative and regulatory considerations underpinning the area of online harms. The Online Harms White Paper was published in 2019, and the Online Safety Bill received its first reading in March 2022. The Online Safety Bill received Royal Assent in October 2023, and is now in law in the UK as the Online Safety Act 2023. This is viewed as a watershed moment for online harms legislation, and it provides for a new regulatory framework to make online services safer for UK residents. In summary, the Act:

- imposes a duty of care on providers regulated by the Act to identify, mitigate, and manage the risks of harm from illegal content and activity, and content and activity that is harmful to children;
- confirms Ofcom as regulator for online safety, with Ofcom being required to issue codes of practice in relation to duties under the Act; and
- places duties on in scope services to have regard to safety by design, and design and operate services in a way to provide higher standards of protection for children, while also ensuring user rights to expression and privacy, and providing transparency and accountability in service provision.

Throughout the recent sectoral analysis research, several stakeholders have noted that clear and definitive legislation and regulation is required on a sustained basis to identify and respond to a range of online harms. The passage of the Online Safety Act may act as a catalyst for enhanced demand for safety tech solutions. This may be both through a regulated basis (where identification, mitigation and response to illegal harms through moderation and forensics may be required), but also in recognition of a market preference to minimise harms such as toxicity, abuse, and fraud across a wide range of sectors and domains.

Since Royal Assent, Ofcom has been working at pace to drive forward its implementation. They are taking a phased approach and have set this out in their [implementation roadmap](#). This will be delivered in three phases:

#### PHASE 1: ILLEGAL CONTENT DUTIES

Ofcom published their consultation on the draft codes of practice and guidance for the illegal content duties in November 2023, which has now closed. These codes will set out the steps companies can take to fulfil their duties and in scope services will either need to follow these, or demonstrate their approach is equally effective. It is expected that Ofcom will submit the final versions of codes and guidance to the Secretary of State for Science, Innovation and Technology to be laid before Parliament for approval, by the end of 2024.

#### PHASE 2: CHILD SAFETY, PORNOGRAPHY AND THE PROTECTION OF WOMEN AND GIRLS.

Ofcom published their consultation on draft guidance for the Part 5 (provider pornography)

duties in December 2023, which has now closed, and in May 2024 published draft codes of practice for the child safety duties. We expect that by Spring 2025 further consultation will also take place on draft guidance on the protection of women and girls.

#### PHASE 3: TRANSPARENCY, USER EMPOWERMENT, AND OTHER DUTIES ON CATEGORISED SERVICES

A small proportion of services will be designated as Category 1 (user-to-user services over a designated threshold), Category 2A (major search services) or Category 2B (other categorised user-to-user services) and will be required to comply with further duties, depending on their category. Ofcom published its advice to Government on these [categorisation thresholds](#) in March 2024. The Secretary of State for Science, Innovation and Technology will consider this advice in developing the regulations required to set the thresholds for the different categories of service.

Ofcom is also working with partners internationally through the Global Online Safety Regulators Network, which brings collaboration from legislated regulators in Australia, Ireland, France, Fiji, Republic of Korea, and South Africa, and the World Economic Forum's Global Coalition for Digital Safety.

The previous UK Safety Tech Sectoral Analysis also recognised the role of wider partners such as the Information Commissioner's Office, with oversight for data protection and the Age Appropriate Design Code, and the Department for Business and Trade in facilitating trade missions between UK safety and security providers and global markets.

The UK has also recognised that advances in Artificial Intelligence will require additional testing and evaluation to ensure AI safety. In November

2023, the UK held the world's first major AI Safety Summit, and launched the AI Safety Institute in recognition that 'AI can be misused to generate disinformation, conduct sophisticated cyberattacks or develop chemical weapons. AI can cause societal harms – there have been examples of AI chatbots encouraging harmful actions, promoting skewed or radical views, and providing biased advice. AI generated content that is highly realistic but false could reduce public trust in information.'

There are several key principles and areas of overlap between the safety tech sector, and those involved in the advancement of AI safety, including:

- **Understanding technology misuse:** Both safety tech and AI safety require a deep understanding of how technologies can be misused to cause harm across a number of areas. Further, safety tech providers have a robust understanding of how to identify and consider potential misuse cases, identify common challenges in defining or identifying harm, and developing approaches to mitigate risks. As set out within this analysis, safety tech providers have been at the forefront of using AI and ML techniques to detect and mitigate online harms such as hate speech, disinformation, and child sexual abuse material (CSAM). Many of these techniques can be applied to areas such as AI generated content, and understanding the movement of content at scale.
- **The role of testing and evaluation:** Regular independent audits and evaluations are essential for both safety tech solutions and AI models to assess their effectiveness, identify issues, and ensure compliance with wider safety standards. There is considerable opportunity to share learning and best practices across these domains to strengthen safety for all users. In recent months, safety

tech providers such as ActiveFence have highlighted the need for applying online safety techniques to areas such as Large Language Models (LLMs), to support enhanced resource allocation to reduce risks relating to hate, harm, misinformation or abuse.

- **Access to data:** The advance of AI in recent years continues to emphasise the need for access to robust, high-quality training data – in addition to understanding how datasets can potentially influence the outputs generated by new models. For example, where LLMs have ingested training data with particular concentration of hateful content regarding particular groups, this may skew outputs towards positions of online hate or racism. Ensuring sufficient access to training, weights, and ensuring regulators can understand how models are performing is critical to mitigate against online harms.
- **Collaborative research and knowledge sharing:** There will be a sustained need for collaboration between safety tech providers and specialists in AI safety. Safety tech providers have extensive experience in areas such as content moderation, harm detection, measurement, and considering ethical, legal, and regulatory frameworks in product design, while AI safety researchers offer deep understanding of models, including their efficacy, efficiency, and access considerations. This will become increasingly important with respect to policy and governance, and responsible use of AI. For example, understanding the benefits and harms from open-source vs closed models, and ensuring equitable access to compute capacity.

These factors place the safety tech sector at a key juncture. Providers will be increasingly focused upon supporting firms to comply with new online safety (and AI) regulations, whilst also ensuring their position can support their customers achieve a positive return through reducing hate or harm on their platforms. Many safety tech providers may also seek to improve the overall safety landscape through working with partners to establish new guidance or enable access to free or low-cost solutions to help tackle core harms, and improve the safety of more platforms. Further, the advancement of AI means that safety tech providers (and the wider AI sector) will be cognisant of the need to continually innovate. This may include new partnerships or mergers between AI platforms and safety tech providers, in recognition of the shared need for AI safety and creating a safer ecosystem at multiple points.

#### SUPPORTING THE SAFETY TECH SECTOR

In recent years, there have been a range of initiatives to support the safety tech sector in the UK, including the establishment of the Online Safety Tech Industry Association, which is the UK body for organisations operating in safety tech.

The Safety Tech Challenge Fund has also supported a range of projects designed to improve the response to child sexual exploitation and abuse online combining innovative approaches developed by safety tech companies, academics and third sector organisations. Each company receives funding to develop their solutions and enhance government and safety tech collaboration in addressing how responsible innovation can put children's safety at the centre of technology design and deployment.

In 2023, DSIT partnered with Home Office, GCHQ and Innovate UK KTN to invest over £350,000 in innovation projects that enhance UK capabilities in protecting children online, focusing on detecting and disrupting the sharing and modification of links to child sexual abuse material (CSAM) and locations facilitating CSAM access, including gateway and torrent sites.

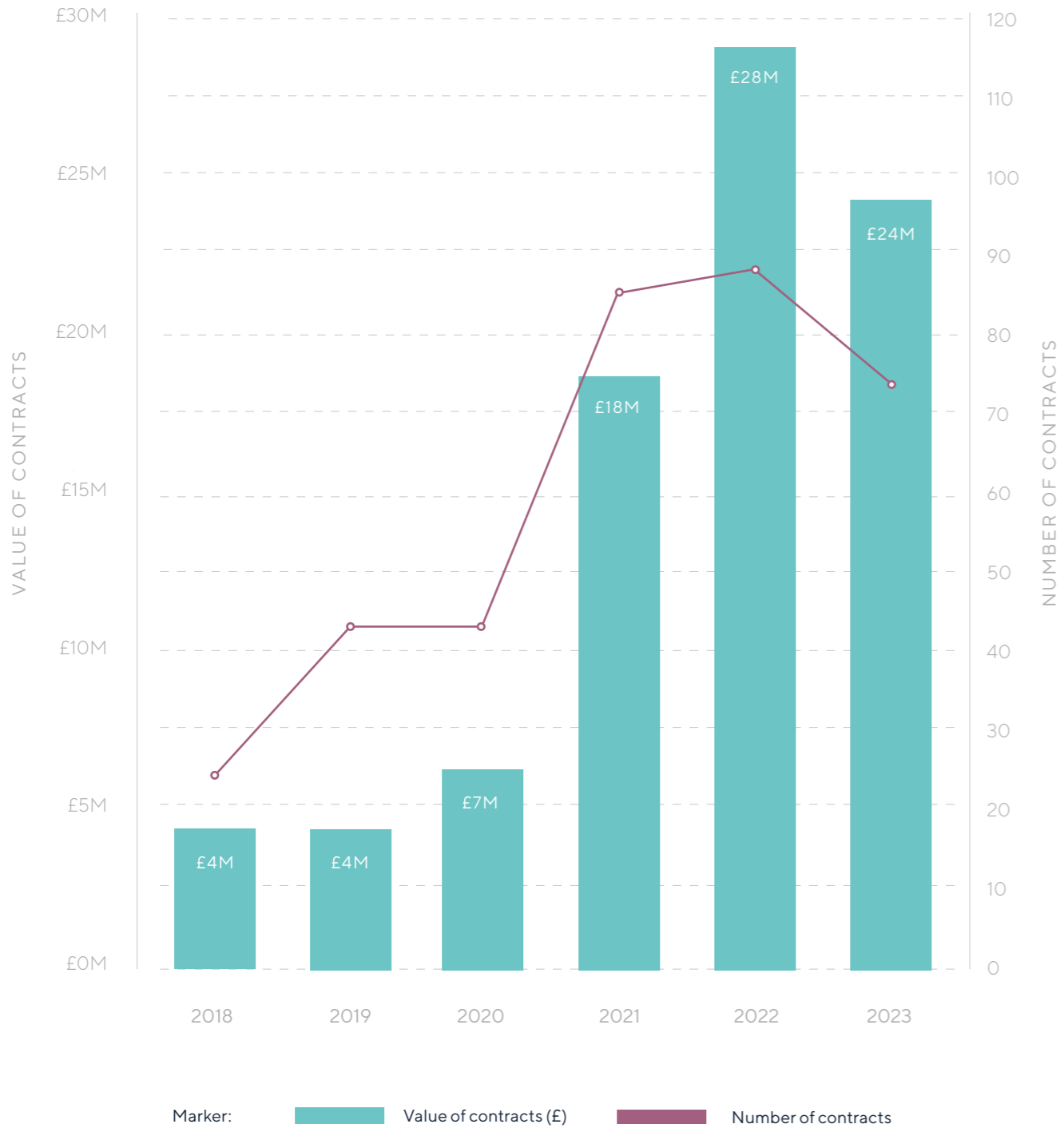
Support for early-stage firms was also made available via the Safety Tech Academy, an initiative that targeted a cohort of early-stage businesses to test ways to support them in creating products and finding routes to market.

#### TRUST AND SAFETY PROCUREMENT

A key-word search of trust and safety language on the Tusell procurement platform has been used to provide an indicative view of public sector demand for safety tech products and services across government, alongside commissioned research projects.

We find sustained demand for safety tech solutions across the public sector, as shown below. We note that 2023 data may have a lag, where authorities report awards retrospectively. Therefore, we expect 2023 demand to be consistent with that seen in 2022. However, this data suggests over 350 contracts awarded between 2018 – 23, with a combined value of £85m.

FIGURE 5: SAFETY TECH PUBLIC PROCUREMENT SPEND (2018 - 2023)



Source: Perspective Economics analysis of Tussell data (2018 - 2022)

The previous sectoral analysis highlighted that key buyers within this market included DSIT (e.g., research and mapping, training, and sector support), Ofcom, Home Office (e.g. research and mapping, and technical services) and Department for Education.

In 2023/24, we find additional contracts issues across buyers such as local government (e.g. for social media monitoring, and support with media literacy and counter-extremism), Cabinet Office (e.g. identifying and responding to disinformation), and police forces.

**KEY BUYERS AND PARTNERSHIPS**

Within this research, we have reviewed company web data (websites and press releases) to explore how the safety tech sector engages with wider industry and partners.

In March 2024, we identified 105 safety tech providers that mentioned 625 customers or partnerships with other businesses or organisations. Overall, this suggests that approximately three-quarters of providers (with a known website) publicly mention indicative customers or partnerships in the market.

For the 38 safety tech businesses that did not have an identified partnership online, these were typically focused in the domains of detecting and responding to illegal content, digital forensics, and OSINT. For many of these businesses, they mention working with law enforcement or government clients, but do not disclose these partnerships due to sensitivities.

For the safety tech businesses that do mention partnerships or customers directly, we find an average of six partnerships per business (median of five). We classify the count of these partnerships by safety tech taxonomy category (best-fit), and the sector of the buyer or partner (classified based on core offering).

TABLE 1: TAXONOMY CLASSIFICATIONS OF THE UK SAFETY TECH SECTOR

TAXONOMY	KEY FINDINGS
<b>Platform level</b>  <b>COUNT</b>  188  <b>PERCENTAGE</b>  30%	<p>The data suggests that safety tech providers that focus on areas such as content moderation or brand safety are much more likely to highlight these partnerships, and highlight how their solutions can support vendors achieve a positive ROI through investing in trust and safety.</p> <p>Review of web data highlights that several providers use testimonials from vendors to articulate these benefits – for example, addressing toxicity at scale, or maximising user engagement on platforms.</p> <p>Typically, customers include a mix of social media and tech firms, but also highlights the reach and usage of platform level solutions by recognised brands across sectors. For example, we find evidence of partnerships between UK safety tech firms and major food and drink brands. Similarly, gaming, media, and banking and finance firms are also highlighted in the partnership data for platform level providers, indicating an increased focus on brand safety, compliance, and moderation.</p> <p>Indicative buyers and partners include major organisations such as Adidas, Airbnb, BBC, Deliveroo, Diageo, EA, Heineken, HSBC, Levi’s, Meta, Peloton, Tesco, Unilever, and Visa.</p>
TAXONOMY	KEY FINDINGS
<b>Age oriented online safety</b>  <b>COUNT</b>  93  <b>PERCENTAGE</b>  15%	<p>Ensuring adequate provision for age-checking and user verification is a key component of online safety, as well as regulatory compliance in areas such as retail and finance. Further, the growth of under-18s online (and over-13) can mean that many online platforms must comply with legislation such as the US Children’s Online Privacy Protection Act (COPPA), which regulates the collection of personal information for children.</p> <p>The data finds significant evidence of safety tech providers either supporting a wide range of firms to comply with privacy regulation e.g. SuperAwesome and Hasbro, as well as innovative forms of user verification e.g. Yoti’s partnership with Meta to verify age on Instagram. There are also several partnerships to help use age and user verification across settings such as physical and online retail, and digital identity provision.</p>

TAXONOMY	KEY FINDINGS
<b>Information governance</b>  <b>COUNT</b>  98  <b>PERCENTAGE</b>  16%	<p>The data highlights an extensive range of partnerships between safety tech firms focused on tackling disinformation, and organisations focused on advertising, marketing, media and branding. For example, safety tech organisations such as NewsGuard and the GDI have strong partnerships with a range of adtech and media organisations to help verify content and provide trust and assurance.</p> <p>Further, there is also evidence of partnerships between multiple safety tech firms in this domain (e.g., data sharing, adoption of shared principles), as well as novel partnerships with charities and social enterprises focusing on areas such as content provenance and authenticity, and media literacy.</p> <p>We also find some evidence of information governance firms associated closely with universities, potentially with a research focus to help inform the identification, measurement, and responses to disinformation. Providers also have a range of partnerships with government, law enforcement, and defence applications – supporting the identification of bad actors and harmful narratives.</p> <p>Examples of buyers and partnerships include Adobe, Microsoft, Integral Ad Science, Salesforce, the Guardian, government departments (UK and US), and YouTube.</p>
TAXONOMY	KEY FINDINGS
<b>System-wide governance</b>  <b>COUNT</b>  82  <b>PERCENTAGE</b>  13%	<p>Online platforms have an obligation to ensure that they can detect, mitigate, report, and respond to illegal content or behaviour. The review of UK safety tech providers highlights strong customer relationships between UK providers and law enforcement bodies, with key buyers including the Home Office, Serious Fraud Office, HMRC and police forces.</p> <p>However, it also highlights major retailers and brands working with providers, particularly to verify transactions and counter fraud. For example, indicative buyers include insurers (e.g., AXA, Allianz), credit services (e.g., Equifax and Experian), security solutions (e.g., G4S), logistics (e.g., DHL) and major retailers.</p>

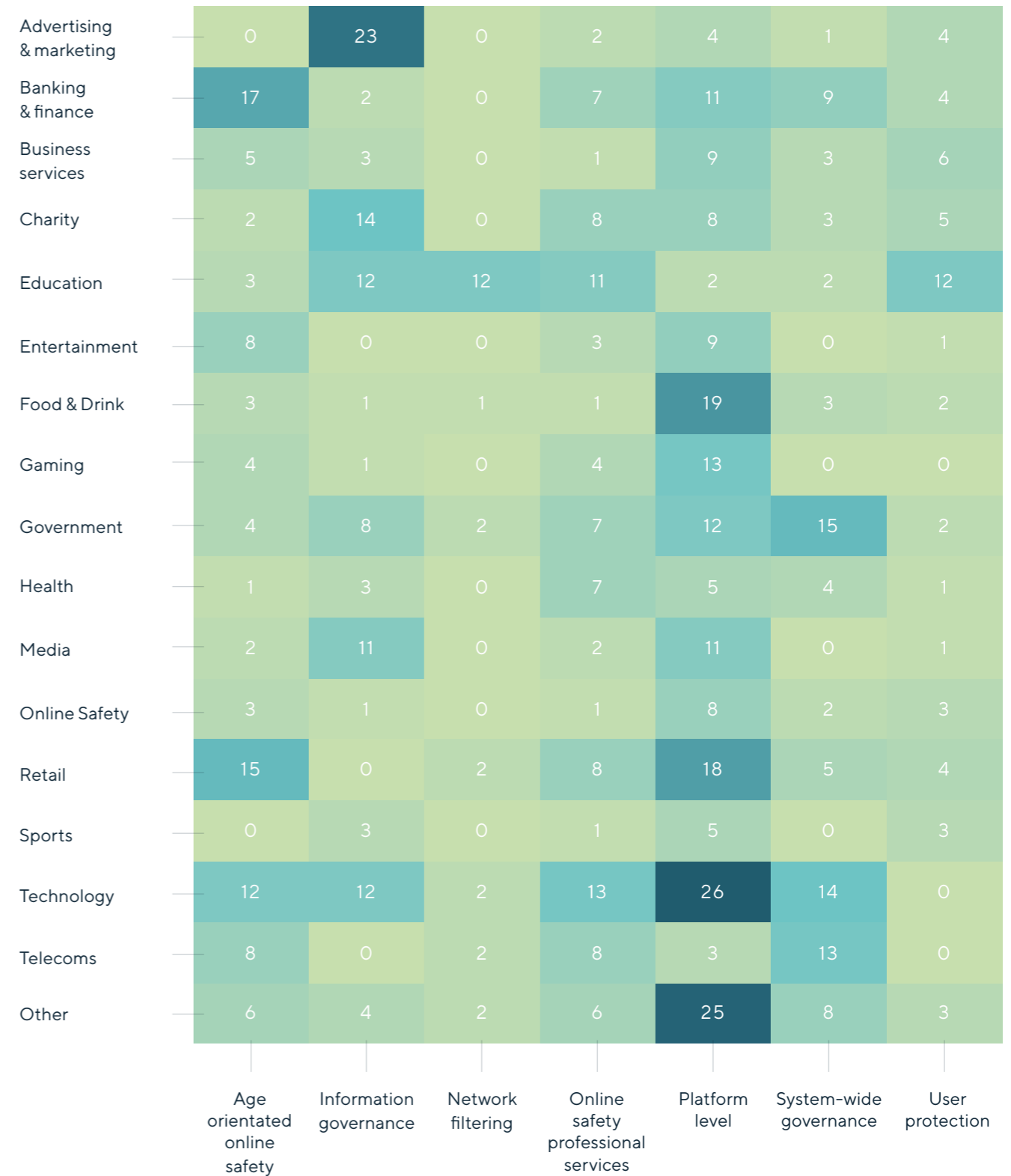
TAXONOMY	COUNT	PERCENTAGE	KEY FINDINGS
User protection	51	8%	This category includes providers typically focusing on endpoint protection on a Business to Consumer (B2C) basis e.g. safety software that can be installed on a device. The research finds safety tech providers working with schools and education settings, in addition to some partnerships with Internet Service Providers (ISPs) and search engines.

TAXONOMY	COUNT	PERCENTAGE	KEY FINDINGS
Network filtering	23	4%	As above, we find some partnerships between filtering providers and schools, and with brands with open WiFi (e.g., retailers, airports, and coffee shops).

Figure 6 highlights the count of partnerships identified between providers and wider sectors. A higher figure is denoted in a darker colour, and sets out where there appears to be market demand for particular solutions. For example, there is a strong overlap between:

- Advertising and marketing firms engaging with information governance safety tech firms to help ensure brand safety, and prevent inadvertent sharing of harmful or hateful content.
- Banking and finance firms engaging with age assurance providers (aligned to digital identity) and platform level firms (to support with moderation in customer processes).
- Large retail, technology, and food and drink brands engaging with platform level providers to support brand safety operations.
- Education providers engaging with network filtering and endpoint protection products and services.
- Government and telecommunications providers working closely with system-wide providers to help identify and respond to illegal harms.

FIGURE 6: MAPPING THE PARTNERSHIPS BETWEEN SAFETY TECH PROVIDERS AND THE WIDER ECONOMY



n = 625 partnerships identified between safety tech providers and wider organisations via web data

## GROWTH EXPECTATIONS & EXPORT ACTIVITIES

Within this research, the team shared an online survey with UK safety tech providers. This survey received 30 responses<sup>2</sup>, which provides some insight into growth patterns, expected trajectories, and nature of income and business models.

This survey found that, in the past twelve months (2023):

- 17 (57%) reported a positive increase in annual revenues. Of these, 6 businesses (20%) reported that revenues had increased by more than 50% in the previous year.
- 8 (27%) reported no significant change in annual revenues.
- 3 (10%) reported a decrease in annual revenues (all by more than 25%), and two businesses were unsure.

Safety tech businesses were also asked to consider how they expected business performance (revenue and employment) to fare in the next twelve months (i.e. all of 2024).

When asked about **revenue** (“Do you expect the revenue of your organisation will increase in the next twelve months? If so, to what extent?”):

- The majority (77%, n=23) of businesses expected revenue to increase. Of these responses:
  - 33% (n=10) expected over 50% annual growth (albeit these responses were primarily from start-ups at pre-revenue or a lower revenue base, with an average revenue of c. £650k).

- 16% (n=5) expected annual revenue growth of >25%, and the remainder (27%, n = 8) were more conservative anticipating growth of >5%.

- 13% of businesses expect no significant change in annual revenues, and 10% were unsure.

Businesses were also asked about **team size** (“Do you expect the size of your team will grow in the next twelve months (e.g. through recruitment)? If so, to what extent?”) in the next twelve months. Two in three businesses (67%) expect team size will increase. However, the majority of businesses with revenue in excess of £1m typically expect team sizes to either increase by no more than 5%, or no significant change expected.

As such, the wider sentiment for 2024 is that revenue may be expected to increase, but employment growth could be more modest than in previous years.

In addition, businesses were also asked about the number of customers they currently have, and if they expected the reach of their business solutions to expand in the next twelve months.

The previous Safety Tech Sectoral Analysis (2023) estimated that over half (54%) of dedicated safety tech companies in the UK had an international presence, either reflected by international offices or export activity. Within this study, we estimate this has increased to 64% (91 providers). This has been driven by increased export activity, and the attractiveness of the UK for international providers setting up in the UK.

BLANK PAGE

<sup>2</sup> As this survey received only 30 responses (out of a potential c. 140), we note this is indicative and may not be fully representative due to sample size. However, it provides useful insight into market conditions.

## 8. Appendices

### APPENDIX A

## Methodology

This section sets out our research methodology for identifying safety tech businesses, and capturing their respective economic contribution. This methodology is consistent with the previous reports.

#### STAGE 1: DATA REVIEW

The research team recognise that safety tech is a challenging sector to define, and will contain businesses which overlap a number of other sub-domains and classifications. To support the development of a sector definition, the research team used the initial definition and sector taxonomy used within the previous studies. This was subsequently subject to minor revisions, and tested through stakeholder workshops to inform a 2023 definition and market taxonomy. This definition has been used in this report.

This helped to:

- Consider any new language or business models used by safety tech providers (e.g. such as public safety, content provenance, brand safety).
- Identify any companies not previously identified, or recent start-ups in safety tech.
- Identify where any platforms are integrating trust and safety solutions, which can have market implications.

The project team also reviewed all known dedicated safety tech firms, excluding any that have ceased trading, as well as over 700 global safety tech businesses in order to explore any international firms registering in the UK. The purpose of this step was to identify any new keywords, companies, or organisations relevant to the safety tech domain, prior to the revised taxonomy and firm identification process.

At this initial stage, the project team identified as many potential input sources or pre-existing lists of firms classified as relevant to a number of agreed high-level terms e.g., content moderation, digital forensics, VAWG, brand safety etc. This supported the project team to build upon the previous year's list, as well as the inclusion of additional providers that fit into the revised taxonomy. Perspective Economics holds a number of datasets and licence agreements to help identify relevant businesses. Analysis was undertaken with Companies House data, Beauhurst, Tussell, web data, and FDI Markets to help identify firms for potential inclusion in the sectoral modelling. The long-list was subsequently reviewed to provide:

- Classify safety tech firms into market categories based on web descriptions (undertaken using a bespoke classifier, and subject to manual review).
- Markers for each of the companies identified to date to highlight broader validation for inclusion within the final safety tech sector list. For example, if a firm has a clear description where they are developing safety tech products, has a team of engineers and data scientists, and has secured external funding or validation – this would be a strong candidate for inclusion. If a firm is only identified in a small number of sources, and / or has a more limited aligned definition – this would be subject to a manual review.

## STAGE 2: TAXONOMY DEVELOPMENT

In 2019, Perspective Economics designed the first safety tech sector taxonomy, in collaboration with DCMS (now DSIT) and industry stakeholders. This recognised a need to set out the core products and services offered, as well as the technology, harms addressed, approach, and benefit to end users. In 2023, Perspective Economics engaged with OSTIA and DSIT to provide an update to the existing taxonomy (see Appendix B).

## STAGE 3: IDENTIFICATION OF FIRMS AND INITIAL MODELLING

Using the updated taxonomy and keywords, the project team searched for additional firms to include within this study. All company data was enhanced using a blend of proprietary sources, web data (using identification algorithms), and Companies House. Sector modelling included an assessment of company accounts, investment data, and estimated team sizes to identify an initial assessment of how the safety tech sector has grown, and helped to identify any gaps for subsequent primary research (consultations).

## STAGE 4: PRIMARY RESEARCH

- Perspective Economics and PUBLIC engaged with over 30 consultees via qualitative interviews and surveys. Consultations included industry, investors, and wider stakeholders in the UK and internationally. Themes consisted of:
  - Discussion of the organisation's engagement with online safety / safety tech / trust and safety or AI.
  - Exploration of relevant themes (growth of the sector, challenges for the adoption of safety tech, where intervention or support might be most appropriate, drivers for growth, potential impact of regulation on the safety tech industry etc). Firms were also asked thematically about AI safety, generative AI, and metaverse (VR/AR technologies) in 2024.
  - Key barriers to business development and growth.
  - Identification of business partnerships or supply chain activities, or engagement with R&D.

## APPENDIX B

# Taxonomy Update

### DEFINITION CONTEXT AND CONSIDERATIONS

The Department for Digital, Culture, Media and Sport (DCMS) (now DSIT) published the Safer Technology Safer Users report in May 2020. This research piece was conducted by Perspective Economics with advisory input from Professor Mary Aiken and Professor Julia Davidson and provides an outline of the online safety technology or safety tech sector profile in the UK.

A number of steps were taken within this original study to define the scope of the safety tech sector. Factors considered include:

- **the technical response utilised to reduce harm**, such as detection and removal of illegal and harmful content, age-appropriate design or age-based safeguarding, detection of disinformation, and or content filtering etc).
- **the type of harm involved that solutions seek to address**, (such as illegal video and image-based content, hate speech, child exploitation, sexual material, personal harm, violence, bullying and harassment etc.)
- **the type and extent of the risk involved**: for example, identifying solutions that can detect and notify platforms and law enforcement about high risk behaviours online.

- **those at most risk of harm**, such as children and young people, those vulnerable to grooming or radicalisation, or those who may not be aware they are exposed to harm e.g., disinformation or deep fakes etc.); and
- **the technologies and approaches deployed to counter the harm** (for example, understanding the technical approaches deployed, for example risk detection and response through artificial intelligence (AI) or machine learning (ML) approaches.

For the purposes of this research, we retain the following definition of the safety tech sector:

**Any organisation involved in developing technology or solutions to facilitate safer online experiences, and to protect users from harmful content, contact or conduct.**

When considering 'online safety' in the broadest sense, the risks can include:

- **Content**: being exposed to illegal, inappropriate, or harmful material;
- **Contact**: being subjected to harmful online interaction with other users; and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.



As such, this research seeks to identify organisations that provide or implement technical products or solutions that either help to:

- Protect users from social harms when using technology and online platforms or services (typically through filtering or controls, or through detection and removal of potentially harmful content); or
- Provide mechanisms to flag, moderate, or intervene in the event of illegal or harmful incidents when using online platforms or services.

For avoidance of doubt, this research seeks to identify and understand organisations that:

- Help trace, **locate and facilitate the removal of illegal content** online;
- Work with social media, gaming, and content providers to **identify harmful behaviour** within their platforms;
- **Monitor, detect and share online harm threats** with industry and law enforcement in real-time;
- Develop **trusted online platforms that are age-appropriate** and provide parental reassurance for when children are online;
- Identify and counter **fraudulent advertising** and scams online;
- Support individuals in maintaining and limiting access to **personal data**, or respond to incidents of doxxing or revenge porn.

- **Verify and assure the age of users;**
- **Actively identify and respond to instances of online harm**, bullying, harassment and abuse;
- **Filter, block and flag harmful content** at a network or device level;
- **Detect and disrupt false, misleading, or harmful narratives;** and
- **Advise and support a community of moderators** to identify and remove harmful content.

As reflected in this list, given the scale of online harms that exist, there are a wide range of technical and applied solutions that can help counter these, and our research seeks to identify the scale and breadth of approaches that exist in the market.

## TAXONOMY

### System-wide level factors

As reflected in this list, given the scale of online harms that exist, there are a wide range of technical and applied solutions that can help counter these, and our research seeks to identify the scale and breadth of approaches that exist in the market.

These organisations help to identify and tackle some of the internet's most harmful content e.g., child sexual abuse and exploitation, terrorist content. This can be achieved through:

- Working closely with law enforcement to assist with investigative capabilities e.g., use of forensic science tools to scan and detect known illegal content using MD5 hashes, or use of AI and tools to identify patterns of harmful behaviour online;
- Maintaining and providing access to technology aimed at preventing the upload, and facilitating the removal of illegal content e.g., the IWF's Hash List (with Microsoft PhotoDNA); and
- Combating abuse or threats with automated content analysis and artificial intelligence e.g., automated detection of terrorist content, including previously unseen material.

Please note that the proposed updates at the system level also consider the harms associated with fraudulent online advertisements and commerce.

### Platform level factors

This refers to organisations that are involved in making online services safer and typically work at the platform level i.e., work alongside social media, gaming, and content providers to improve safety and behaviour within their platforms. These have been segmented into the sub-categories, outlined in the subsections below.

#### Platform governance

These organisations are focused upon helping providers of online content to govern their offering with respect to illegal content. Whilst there is some overlap with 'System Governance', this is more focused on organisations that help to tackle issues such as:

- Embedding prevention mechanisms e.g., using machine learning to prohibit the production of indecent underage imagery on social media platforms;
- Identifying and blocking harmful images and videos in real-time; and
- Identifying child abuse or grooming in conversations.

### Platform moderation and monitoring

These organisations also help providers of online content to monitor and moderate behaviour and content posted within their platforms. This is typically focused upon reducing harmful content or behaviour e.g., offensive language, bullying, or toxic content, fraudulent online advertisements and commerce. This can include:

- Moderation and monitoring of content e.g., pre-moderation or post-moderation of content, undertaken by automated content analysis and / or humans;
- Chat moderation e.g., identifying and removing users subject to language or words used; and
- Behavioural Monitoring e.g., identifying good and bad behaviour, typically using Natural Language Processing within online communities.

### Age orientated online safety

These organisations seek to support online content providers in ensuring that their platforms are either:

- Age-appropriate and increase the privacy of children online (e.g., compliant with GDPR-K, or that the content and access requirements are suitable should the website or app be targeted at under-18s, thereby ensuring 'safety by design'), or provide
- Age assurance services (i.e., help companies to validate and confirm that only particular age groups can access particular content).

### Endpoint level factors

This refers to organisations that provide products or services that help to ensure that the device being utilised by the end-user is suitably secure with respect to online safety. This focuses upon online safety solutions (i.e., ensuring that the user's risks with respect to content, conduct, and contact are reduced). It does not include endpoint protection from viruses, malware, or adware – which are covered by 'cyber security'. User protection at the endpoint level can be segmented into two main categories.

#### User initiated protection (user, parental and device-based)

This includes organisations that provide products or services that can be installed on devices to help secure the end-user from online harms (typically a parent or guardian installing on behalf of a child). The underlying ambition is to create a safer online experience for the user e.g., through safeguarding assistants, oversight of social media content, or through monitoring of a child's digital or online behaviour and interaction with other users. Where deployed, these solutions can help to prevent issues relating to sexting, grooming, bullying, harassment, abuse, or aggression. Solutions may also support users in promoting awareness of personal data rights and / or preventing public access to private information (where consent is not provided) e.g., supporting those affected by 'revenge porn'

### Network filtering

This includes organisations involved in providing products or services that actively filter content (e.g., through white-listing or black-listing, or through actively blocking content perceived to be harmful or illegal). This can often include solutions provided to schools or home users to filter content for users.

### Information environment level factors

This refers to organisations that actively detect and disrupt false, misleading and / or harmful narratives.

### Information governance

This includes tackling misinformation and disinformation through the provision of fact checking and disinformation research and disruption. Organisations within this space seek to ensure citizen information accuracy and facilitate trust in the information environment and wider society.

### Online safety professional services

This includes organisations typically involved in supporting the design, implementation and testing of online safety through the provision of compliance services, research, frameworks and methodologies for auditing, evaluating or mitigating potential harms, and help to enable the development of safer online communities.

Further, this analysis has also sought to identify organisations involved in supporting the development and scaling of online safety products and services but do so in an advocacy capacity e.g., civil society organisations.



#SAFETYTECH

**Perspective Economics**

48-60 High Street

Belfast

BT1 2BE

[www.perspectiveeconomics.com](http://www.perspectiveeconomics.com)