Government
Social Research

Cyber Explorers Pilot Evaluation

Final Report

December 2022

Authors: Ecorys UK and Perspective Economics

Contents

List of figures

List of tables

Executive Summary

The Cyber Explorers programme

The Department for Digital, Culture, Media and Sport (DCMS) contracted QA Ltd to deliver Cyber Explorers, which ran as a six-month pilot. The programme launched on 23 February 2022 and involved the development and delivery of an online programme of cyber security education and skills, and careers inspiration to young people across the UK, aged 11-14 years. The programme was rolled out as part of the government's ambition for cyber skills set out in the National Cyber Strategy and aimed to equip young people with the digital awareness and skills they need to enable them to pursue a career path in the sector. The pilot launched on 23 February 2022 with content being released in stages. The final modules were released in June 2022.

Participation

- 22,778 learners registered for Cyber Explorers.
- The programme exceeded the target for female participation (49% against a target of 25%).
- The programme exceeded the target for learners based in schools outside of London and the South East (79% against a target of 50%).
- The programme exceeded the target for registrations from schools in the three most deprived deciles (21% against a target of 15%) and was slightly under target for registrations from schools in the five most deprived deciles (32% against a target of 40%).
- Most registrations came from schools based in non-pilot areas (89%).
- Across the UK regions, areas such as the South West, Northern Ireland, and Yorkshire and the Humber have seen particularly strong sign-ups in relation to their population size. The East Midlands received a much smaller number of registrations compared to other regions, and may benefit from further targeted marketing or support in future.
- Recommendations to increase registrations and engagement in pilot areas include reviewing targets, contracts, and monitoring processes with delivery partners; the delivery provider having direct contact with schools, utilising local networks (including regional champions such as UKC3 and regional cyber crime units); collecting regular feedback from schools to address barriers such as a lack of time and resources and offering a self-registration option to reduce administrative burden on educators.

Engagement

- Feedback suggested that learners enjoyed the content and increased their knowledge of cyber security. Educators and learners found the platform engaging and appealing, highlighting the diverse range of characters and interactive nature of the content.
- Although schools registered 22,778 learners on the platform, only 8,668 learners subsequently logged in themselves and completed a module. The way in which Cyber Explorers was used in schools may impact the engagement data collected. For example, it may be that some schools operate one computer terminal between two in their computer suites, and that some schools present content from a single teacher controlled terminal in the classroom, making it difficult to measure engagement from learner login data. In future more data needs to be collected to allow a better assessment of learner engagement.
- Only 434 registered learners completed six out of seven available modules. This was not unexpected as the final modules were only made available on the platform in June, at the tail end of the academic year. Feedback from all stakeholders suggests that module completion rates were hampered by the fact that the launch was in the second half of the school year, which meant that the programme ran at an inconvenient time in the school year, for example during busy exam periods and approaching the summer holidays.
- Educators mainly delivered, or planned to deliver, the programme in computer science classes but a minor theme was that the programme worked well as homework tasks or as the focus of an extra-curricular club. A major theme was that educators would like to see further curriculum mapping and an improved dashboard functionality to monitor learners' progress.
- Recommendations to increase engagement include reviewing content to ensure it is suitable for older age groups, curriculum mapping to wider subject areas, as well as computing subjects, adding more hands-on elements such as quizzes and games, offering incremental increases in difficulty, and use of inspirational role models from industry to bring sessions to life.

Outcomes and impact

- Survey data suggested that there are indications that the programme has increased learners' understanding, knowledge and skills relating to cyber security. Learners found the content interesting and noted that they enjoyed learning about topics beyond what they would cover in lessons.

- It was not possible to detect the impact on learners' interest in cyber security as a study subject or as a career. This may be due to small sample sizes and low levels of engagement with the content.
- Qualitative feedback suggested that some learners had developed a better understanding of how cyber security related to a range of job roles, and some expressed a new interest in pursuing this further when they were older.
- It is recommended that changes are made to ongoing data collection to assess outcomes in the short and longer term. Firstly, it is suggested to include further data validation on learner characteristics to attain more complete data. It is also important that measures are implemented to ensure learners complete data collection exercises in the correct order and at the appropriate time point to provide a larger and more robust sample for impact evaluation to be completed in future.

Introduction

In January 2022, the Department for Digital, Culture, Media and Sport (DCMS) commissioned Ecorys and Perspective Economics to evaluate the Cyber Skills Programme, consisting of the Cyber Explorers and the Adult Skills pilot. This report covers the pilot of Cyber Explorers that was launched in February 2022. It incorporates results from several strands of data collection, including feedback from learners who participated in the programme, educators, delivery and industry partners, and the delivery provider. Management Information (MI) was provided by the delivery provider.

Policy context

In 2016, the government launched its National Cyber Security Strategy[1] (NCSS), along with the £1.9 billion National Cyber Security Programme (NCSP). This investment has supported innovative policy and interventions to build economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment. A new National Cyber Strategy[2] was published in 2022, which sets out the vision that the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals. Among other initiatives, this outlines the need for training programmes working to ensure that everyone can join the cyber workforce, tackling inequality in the sector where only 16% of the workforce are female, and only 3% of senior roles are held by women and ethnic minorities.[3]

To explore the demand for capability, the government commissions annual research to define cyber security skills gaps and shortages[4]. The study found that half of all UK businesses (51%) have a basic technical cyber security skills gap (up from 50% in 2021) and 33% of UK businesses have an advanced cyber security skills gap (up from 30% in 2019). Given the inherent nature of cyber threats to a digital economy, such a capability gap is not sustainable.

The Cyber Explorers programme

DCMS contracted QA Ltd to deliver the Cyber Skills & Careers Inspiration Programme for Young People, marketed as Cyber Explorers. The programme ran as a six-month pilot

1 National Cyber Security Strategy https://www.gov.uk/government/publications/national-cyber-security strategy-2016-to-2021

2 National Cyber Strategy, 2022 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

3 HMG, Cyber security skills in the UK labour market (2021) Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973802/Ipsos_MORI_Cyber_Skills_in_the_UK_2021_v1.pdf

4 Cyber Security Skills in the UK Labour Market 2022. Findings Report. May 2022. Ipsos Mori.

which launched on 23 February 2022. The Cyber Explorers programme has involved the development and delivery of an online programme of cyber security education and skills, and careers inspiration to young people across the UK, aged 11- 14 years. The programme aims to:

- increase the uptake of computer science and related digital subjects at age 14 and beyond
- increase awareness by teachers of cyber and digital learning opportunities
- increase the numbers of young people across the UK leaving full-time education with digital and cyber skills and increasing the number who have been inspired to take up a career in cyber security, or other digital technology roles
- increase visibility of Cyber Careers and the routes into the sector, including the benefits of working in Cyber, for pupils and their teachers, parents and school leaders
- secure the foundation for long-term employer engagement in the digital and cyber skills agenda, contributing to the UK's need to protect against future cyber threats
- increase engagement with and involvement by hard-to reach groups in Cyber Security including girls, ethnic minorities and those from a disadvantaged Socio-Economic Background
- increase penetration of extra-curricular Cyber Security learning in State Schools
- increase engagement with local Cyber Security ecosystems

The timeline for delivery was extended relative to the original timings listed in the evaluation tender documents. This was due to a decision by the Supplier to change the system infrastructure (registration platform and database), which needed to be built from scratch and independently assessed (via the CHECK accreditation process). DCMS agreed with this proposal. The platform was initially expected to launch at the end of October 2021 but this ultimately took place on 23 February 2022. Content was released in stages, with the final modules released in June 2022.

The platform itself is an online, browser-based learning platform designed to showcase how digital, computing and cyber security skills are integral to successful career paths. This is delivered through a gamified learning experience consisting of eight modules of content: inspiration, 'Hang Outs', challenges and a final 'Save the City' task. A full overview of the content is provided in Annex Four. Teachers are required to register an account on the portal before enrolling students. Once their details have been verified by QA, they can register students individually or through a bulk upload. Educators are asked to confirm that parents/guardians have provided consent for the child to participate in the Cyber Explorers Programme. The programme also involved a national marketing

campaign consisting of promotional emails to schools, social media campaigns, LinkedIn advertising.

The programme also uses a delivery partner model to focus promotional activity on five pilot areas (Bradford, Birmingham, Newry, Newport, and Inverclyde) with a strong emphasis on diversity and inclusion. A summary of the targets for each delivery partner are provided below.

Table 1: Summary of delivery partner targets

Delivery partner and region	Summary of targets
Partner 1 - Birmingham	Run campaign and events to reach 1000 students and register 500 on to the platform, through careers expo, assemblies, and faith classes
Partner 2 - Bradford and Inverclyde	Provide role model speakers to go into three schools in Bradford, and three in Inverclyde. To deliver a 'Cyber Hackathon' event in one school in Inverclyde
Partner 3 – Newry	Work with six schools to deliver Discovery Days (1/2 day sessions in each school, including role model speakers and Cyber Explorers content) and engage with 453 students
Partner 4 – Newport	Reach a target enrolment figure of 453 students through outreach activities and social media campaigns
Partner 5 - Birmingham	Conduct teacher awareness raising, present Cyber Explorers at their Teacher and Advisers Conference, and run two school events for between 50 and 100 students
Partner 6 – Bradford	Work with one secondary school to introduce cyber security as a career choice and organise related activities to enable QA to deliver Cyber Explorers content

Source: Background information from QA

The evaluation

This section summarises the evaluation implemented by Ecorys. This includes a brief overview of the evaluation strands and data collection achieved; the scope of this report; and the data limitations relating to the quantitative and qualitative findings. The full list of research questions is available in Annex Two.

Aim

The aims of the evaluation were to:

- understand if the intervention was effective and what short term impact the intervention had as well as the likelihood of achieving any long term impacts.
- understand the impact of the intervention so that it can be compared to other similar interventions to understand best ways to intervene in this area and what can be learned from how the intervention was delivered.

Methodology

The evaluation took a mixed methods approach involving both quantitative and qualitative data collection. The following table shows the main strands of data collection, the sample sizes achieved for each as of 21 July 2022. A detailed overview of the methodology is provided in Annex One.

Table 2: Data Collection

Data collection	Sample achieved (22/7/22)
MI and Registration Data	Learner registrations: 22,778 Educator registrations: 2,039
School case studies: interviews with educators and learners	16 teacher interviews, Three focus groups with c. 20 students each (60 learners total) Online survey responses from 245 learners
Interviews with industry partners/delivery partners	11
Interviews with policy stakeholders	8
Interviews with delivery provider	5
QA Baseline learner survey	146 (138 after data quality control)
QA Follow-up learner survey	Engaged: 0 Unengaged: 2 Total: 2
QA Baseline educator survey	78
QA Follow-up educator survey	Engaged: 8 Unengaged: 3 Total: 11
System questions[5] (pre)	5,611
System questions (post)	87
Counterfactual pre survey	2,014
Counterfactual post survey	Post wave 1: 581 Post wave 2: 434 Total: 1015

[5] "System Questions" or "SQ" are three core questions regarding learners' perceptions on their own understanding of cyber security, their cyber skills, and their likelihood to pursue further cyber-related qualifications. These questions were embedded in the Cyber Explorers platform (for more detail please see Annex One)

Report

This report provides feedback from stakeholders across the overall Theory of Change (see Appendix Three) and covers programme delivery, student and educator outcomes and impact and a final section outlining conclusions and recommendations.

Data limitations

This section outlines the main data limitations relating to the qualitative and quantitative findings.

- **Small sample sizes:** Sample sizes in the learner survey, the educator survey and the System Questions were very small, mainly due to the lack of post data. Post samples were 2, 11, and 87 respectively, which were also not entirely usable as "users", as not all of them were engaged with the programme. As expected, samples of System Questions respondents were higher than those of the learner and educator surveys, as they were embedded in the platform, however the System Questions sample was also lower than expected due to practical issues with the platform. One of the key issues was that not all of the learning content was available from the start, resulting in many students responding to the initial questions (n=5,611) but then waiting for the rest of the content to be uploaded. This resulted in a drop in engagement, while it also coincided with summer holidays when less students are expected to respond to surveys like this (resulting in only 68 students coming back to fill the post questions). A second reason for the reduced sample was that the phrasing and position of the System Questions within the platform led to students filling the pre and post questions in the wrong order. For example, some students only filled the post questions, other students filled the post questions before the pre-, and others filled both at the same time, meaning that none of them can be used for pre-post analysis. This resulted in a sample of only 23 students who filled the pre and post questions in the right order and went on to engage with the platform.
- **Self-reported outcomes and interpretation**: Outcomes data is based on subjective, self-reported data rather than more objective data, such as a test score. This may lead to bias. For example, respondents might overestimate their knowledge prior to enrolling in the programme, as they are not aware of gaps in their knowledge until these are highlighted by taking part in the programme.
- **Sub-group impact analysis was not possible due the small sample size** (a maximum of n=23 matched pre-post respondents). An impact analysis on different sub-groups would reduce our sample (and thus our ability to detect impact) even further, as we would have to divide it into smaller sub-samples (for example 12 males and 11 females to test the impact on different genders). This was also not possible for specific sub-groups as in some cases there was no available

information. For example, all 23 respondents in our impact analysis are from non-pilot areas, which means that impact between pilot and non-pilot areas cannot be tested with the current data.

- **Low levels of programme engagement:** At the time of data collection, educators and learners were still able to register and take part in Cyber Explorers, and in some cases not all Cyber Explorers content was live. While KPIs and targets were based on six months of programme delivery, delays to programme delivery meant that the final data available for this analysis was based on five months in the market (using a cut-off date of 21 July 2022). It is possible that the profile of those registering and taking part in data collection, and perceptions of outcomes will change as new data is collected in future phases of the programme. For example, all case study visits were conducted as part of introductory sessions delivered by QA, meaning educators and learners had not yet had the opportunity to complete all available content to be able to comment extensively on the content of the programme and outcomes derived from completing it.

Programme participation

Registrations

- 22,778 learners registered for Cyber Explorers
- The programme exceeded the target for female registrations (49% against a target of 25%)
- The programme exceeded the target for registrations from schools outside of London and the South East (79% against a target of 50%)
- The programme exceeded the target for registrations from schools in the three most deprived deciles (21% against a target of 15%) and was slightly under target for registrations from schools in the five most deprived deciles (32% against a target of 40%)
- Most registrations came from schools based in non-pilot areas (89%)

Engagement

- Feedback suggested that learners enjoyed the content and increased their knowledge of cyber security. Educators and learners found the platform engaging and appealing, highlighting the diverse range of characters and interactive nature of the content.
- Although schools registered 22,778 learners on the platform, only 8,668 learners subsequently logged in themselves and completed a module. The way in which Cyber Explorers was used in schools may impact the engagement data collected. In future more data needs to be collected to allow a better assessment of learner engagement.
- Only 434 registered learners completed six out of seven available modules. This was not unexpected as the final modules were only made available on the platform in June, at the tail end of the academic year. Feedback from all stakeholders suggests that module completion rates were hampered by the fact that the launch was in the second half of the school year, which meant that the programme ran at an inconvenient time in the school year, for example during busy exam periods and approaching the summer holidays.
- Educators mainly delivered, or planned to deliver, the programme in computer science classes but a minor theme was that the programme worked well as homework tasks or as the focus of an extra-curricular club.
- A lower proportion of learners from deprived areas appear to go on to log on to the platform and answer System Questions, suggesting potential drop-out post-

registration for this group.

Recommendations

The following recommendations were made to increase registrations and engagement in pilot areas:

- Review targets, contracts, and monitoring processes with delivery partners to manage expectations of all parties and ensure that consistent monitoring information is collected
- Include more direct contact between the delivery provider and schools to ensure that registrations result in engagement
- Utilise local networks to promote the programme widely
- Continue to collect regular feedback from schools to address barriers such as a lack of time and resources
- Introduce a self-registration option to reduce administrative burden on educators

This section examines total participation numbers across the programme and also examines diversity across key demographic characteristics, based on targets relating to age, gender, pilot area participation, geographic spread of participation, and deprivation.

Student and educator registrations

This section provides basic details on learner participation. This includes a review of the MI data available, in addition to early qualitative findings regarding learner enrolment, participation, and sentiment.

As of 21 July 2022, there are 22,778 learners and 2,039 educators registered on the platform. The formal KPI was to achieve 30,000 learner registrations by 23 August 2022, with an indicative aim to achieve 20,000 learner registrations by the end of June 2022.

Demographic data was examined for the 22,778 learners and 2,039 educators registered at the time of analysis. The analysis includes the proportion of learners who attend a school in the three and five most deprived deciles, based on data from the Index of Multiple Deprivation. This data is based on the school postcode, not individual postcode, so does not reflect individual learner deprivation levels.

The following table shows the key data for learners who registered (against target) and for educators (no targets were set). Data comes from a census of all learners and educators who registered.

Table 3: Learner and educator registrations against targets

	Learner (n=22,778)	Learner: Target	Educator (n=2,039)	Educator: Target
Age	No KPI for age but for learners whose age was provided at registration (n=20,866), age breakdown as follows: 11: 616 (3%) 12: 5,828 (28%) 13: 7,141 (34%) 14: 7,281 (35%)	Targeted at 11-14 year olds	No KPI	No KPI
Gender	Male: 8,446 (51%) Female: 8,209 (49%) Other: 41 (<1%) Did not provide: 6,086	25% female participation	No KPI	No KPI
Location	**Pilot Area:** 2,551 (11%) (of which): Newport: 1,121 Birmingham: 789 Newry: 401 Inverclyde: 159 Bradford: 81 **Non-Pilot Area:** 20,231 (89%)	7,500 (out of 30,000 total) must be regularly engaged with the platform and programme within the pilot areas.	**Pilot Areas**: 80 (4%) (of which): Birmingham: 38 Bradford: 19 Inverclyde: 9 Newport: 8 Newry: 6 **Non-Pilot Area:** 1,959 (96%)	Number of state funded schools participating in the programme within the regional pilot areas to be 80% of the total within each pilot region within six months of the campaign launch.
Outside of London and the South East	18,042 (79%)	50%	As learner (based on school postcode)	50%
At a school in the three and five most deprived deciles	Three most deprived: 4,764 (21%) Five most deprived: 7,372 (32%)	Three most deprived: 15% Five most deprived: 40%	As learner (based on school postcode)	Three most deprived: 15% Five most deprived: 40%

Source: Ecorys analysis of QA MI data

The above figures on learner registrations (n=22,778) suggest the following:

Age

No target was set for the age of learners, although the programme was aimed at learners aged 11-14 years. Registration data suggests that there were more learners aged 13 or 14 compared to the younger ages. This may suggest that educators were more interested in introducing extra-curricular activities for this age group or it may reflect the year groups taught by educators who responded to marketing materials, for example if more Year 9 and 10 and equivalent educators were on mailing lists. Further data would be required to explore the reasons for this. A major theme from qualitative feedback from educators and learners was that the style and content, for example the colours and animation style, was perceived as more suitable for younger students, and they would like to see more content aimed at learners aged 13 and above.

Gender

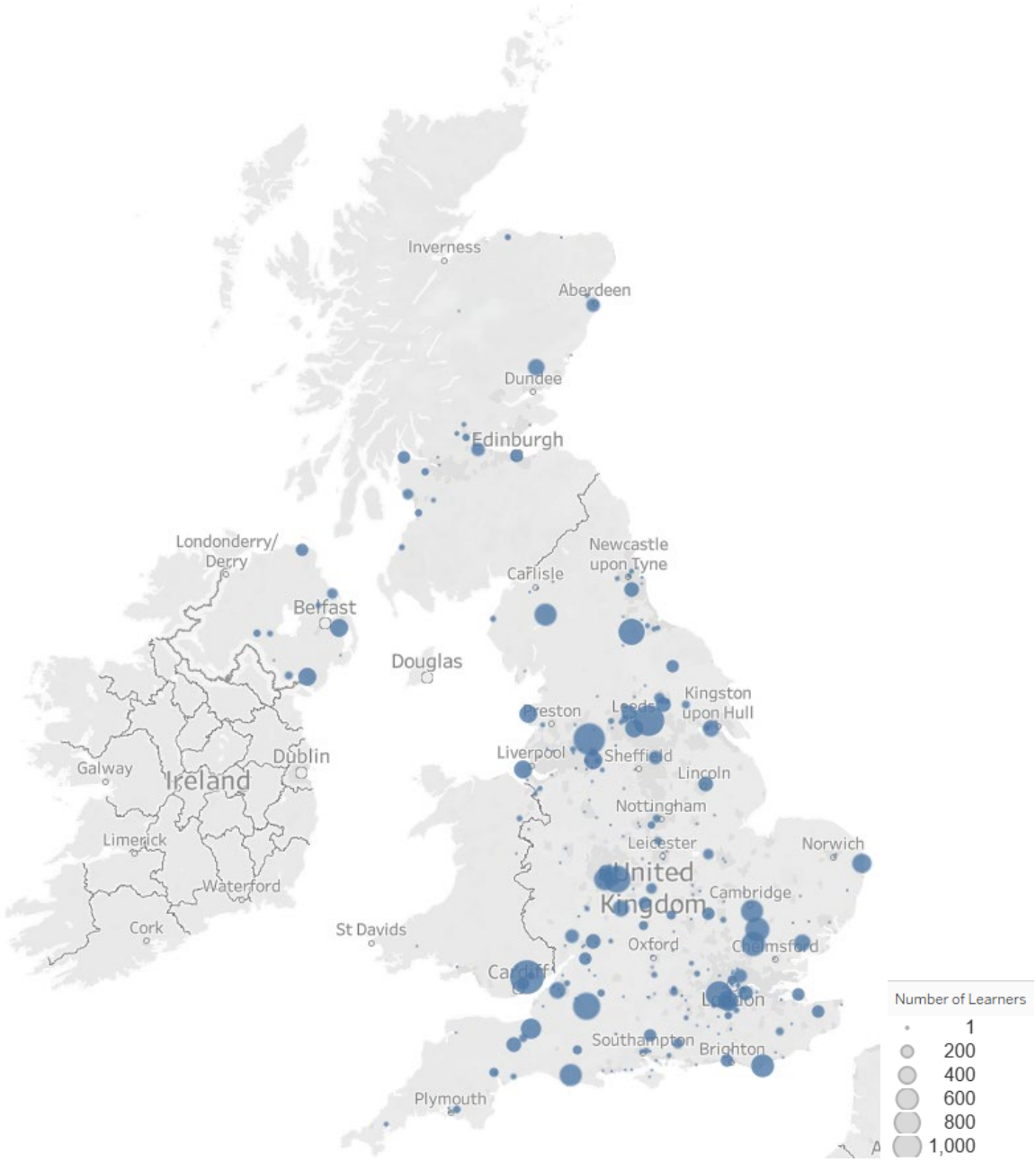
Cyber Explorers appears to have exceeded its target for female participation based on registrations, with 49% of learners registering identifying as female (KPI of 25%).

Location

There was significant variance in learner registrations between pilot areas, with relatively low levels in Inverclyde, Bradford, and Birmingham (given the large size of the latter), and higher in Newport and Newry. Uptake may have been affected by prior participation with initiatives such as CyberFirst Schools, which was limited in Inverclyde and Bradford.

Cyber Explorers exceeded its target for the proportion of learners outside of London and the South East. Figure 1 below shows a map of registrations, indicating take-up of the programme across the UK. In total, the registrations were achieved from more than 308 postcode areas, demonstrating the breadth and reach particularly outside of London and the South East. Overall, the total number of registrations has been driven by a smaller number of postcode areas with higher registration levels. For example, there are 28 postcode areas with more than 250 registrations. 89% of registrations were outside of a pilot area, with high demand in areas such as Rochdale, Leeds, Wiltshire, Solihull, Darlington, Hertfordshire, and Essex.

Figure 1: Location of Registrations across the UK



Source: Ecorys analysis of QA data

Exploring registrations by each of the twelve UK regions suggests the following breakdown of take-up:

Table 4: Registrations across the UK (absolute and relative)

Region	Learner Registrations	Percentage of Registrations	Estimated Percentage of UK Population	Location Quotient[6]
Northern Ireland	1,073	4.70%	2.80%	1.68
South West	3,172	13.90%	8.40%	1.65
Yorkshire and the Humber	2,768	12.20%	8.20%	1.49
Wales	1,386	6.10%	4.70%	1.3
North East	1,039	4.60%	4.00%	1.15
North West	2,689	11.80%	11.00%	1.07
West Midlands	2,136	9.40%	8.90%	1.06
South East	2,841	12.50%	13.70%	0.91
East of England	1,772	7.80%	9.30%	0.83
Scotland	1,393	6.10%	8.10%	0.75
London	1,898	8.30%	13.40%	0.62
East Midlands	585	2.60%	7.30%	0.35
Other / unknown	26	0.10%		

Source: Ecorys analysis of QA data

This highlights that across the UK regions, areas such as the South West, Northern Ireland, and Yorkshire and the Humber have seen particularly strong sign-ups in relation to their population size. Wales, the North West, the West Midlands, and the North East have also performed relatively well with respect to regional spread. Registrations are proportionately lower in London and South East, albeit this is partially due to design of the programme to concentrate on pilots outside of those areas. Registrations are also more mixed in areas such as Scotland, which did contain a pilot in Inverclyde but has seen lower than anticipated sign-ups particularly in areas such as Glasgow and Edinburgh. The East Midlands has received a much smaller number of registrations

[6] This measure explores the relationship between the percentage of registrations in an area relative to the size of the population. For example, if a region has 10% of the registrations, and 10% of the population – then this would receive a Location Quotient of 1 (i.e., the number of registrations is expected in line with the population size). If an LQ exceeds 1, this suggests a high concentration of activity in the region. If an LQ is below 1, this suggests a lower concentration of activity relative to the region's size.

compared to other regions, and may benefit from further targeted marketing or support in future.

Enablers and barriers to recruitment in pilot areas

Interviews with delivery partners and the delivery provider suggested a number of barriers to participation in pilot areas. A major theme was the condensed timelines which made it difficult to engage schools as they had already finalised their timetables for the year. This was a challenge across locations, but it was noted that recruitment was particularly difficult in schools in areas of deprivation. Through their ongoing engagement work, including focus groups with educators, the delivery provider recognised that educators in these areas were more likely to describe themselves as time-poor and often had competing priorities which made it difficult to implement a new, extra-curricular programme. For example, they found that parents/carers in these areas were perceived by educators as being less actively involved with their child's education, so it was harder to get parental consent for extra-curricular programmes. It is recommended that in future phases, the delivery provider continues to engage regularly with schools to ensure that barriers such as lack of time and resources can be addressed, and additional resources are available to support schools in more deprived areas.

A major theme from interviews with the delivery provider was that QA-led sessions in schools were more effective in generating registrations than large scale events led by delivery partners, although feedback suggests they can support wider aims such as awareness of cyber security careers. For example, a careers fair in one of the pilot areas received positive feedback from attendees in terms of raising awareness of careers in tech more generally but this is difficult to measure and did not see a strong return in terms of platform registrations. A minor theme was that using an external delivery partner felt like a barrier to the delivery provider engaging with schools directly and getting them registered on the platform. For future phases, it is recommended that the delivery provider's own support staff can liaise with schools directly. A minor theme was that some delivery partners felt restricted by rigorous sign-off processes and would have preferred more creative freedom when running marketing campaigns with their audiences, although they recognised the importance of consistent branding. In addition, some partners reported that it was not clear from the outset who the target audiences would be for the campaign, so they initially planned activities and communications for parents/carers and learners, but it later became clear that all activity should be focused on educators. It is recommended that more specific guidance and contracts are issued to delivery partners to manage expectations of all parties, ensure that appropriate targets are set and consistent monitoring information is collected.

Enablers to successful promotion and recruitment in pilot areas included the use of inspirational role models from industry to bring sessions to life and run hands-on sessions with students. A major theme was the importance of using a diverse range of speakers that learners could relate to and to show how the skills and knowledge covered in Cyber Explorers can be applied to different job roles. Delivery and industry partners

suggested that the programme could go further in providing a clear pathway into careers in cyber security, for example resources that suggest possible roles based on learners' skills and areas of interest (such as coding or encryption) and next steps on how to pursue those roles. A minor theme was that delivering sessions to smaller groups was more effective than talks to whole year groups as it allowed more time for meaningful interactions with learners and the opportunity to ask questions. It was suggested that briefing materials could be provided to delivery partners that suggest activities and resources to engage educators and students, and mechanisms put in place to share best practice in terms of activities that have worked well in different areas. Interviews with the delivery provider and policy stakeholders suggested that more could be done to utilise existing networks, local contacts and knowledge to promote the programme in pilot areas. It was noted that DCMS regional leads were key in making introductions to relevant stakeholders, such as UKC3[7] and regional cyber crime units, and they should be engaged as early as possible in the process.

Deprivation

Registration data shows the programme achieved the KPI for reaching young people attending schools situated in the three most deprived areas (21% compared to the 15% KPI), but not the five most deprived deciles (35% compared to 40%). As outlined in the User characteristics section, a lower proportion from the deprived areas appear to go on to log on and answer System Questions, suggesting potential drop-out post-registration for this group.

Engagement and module completion

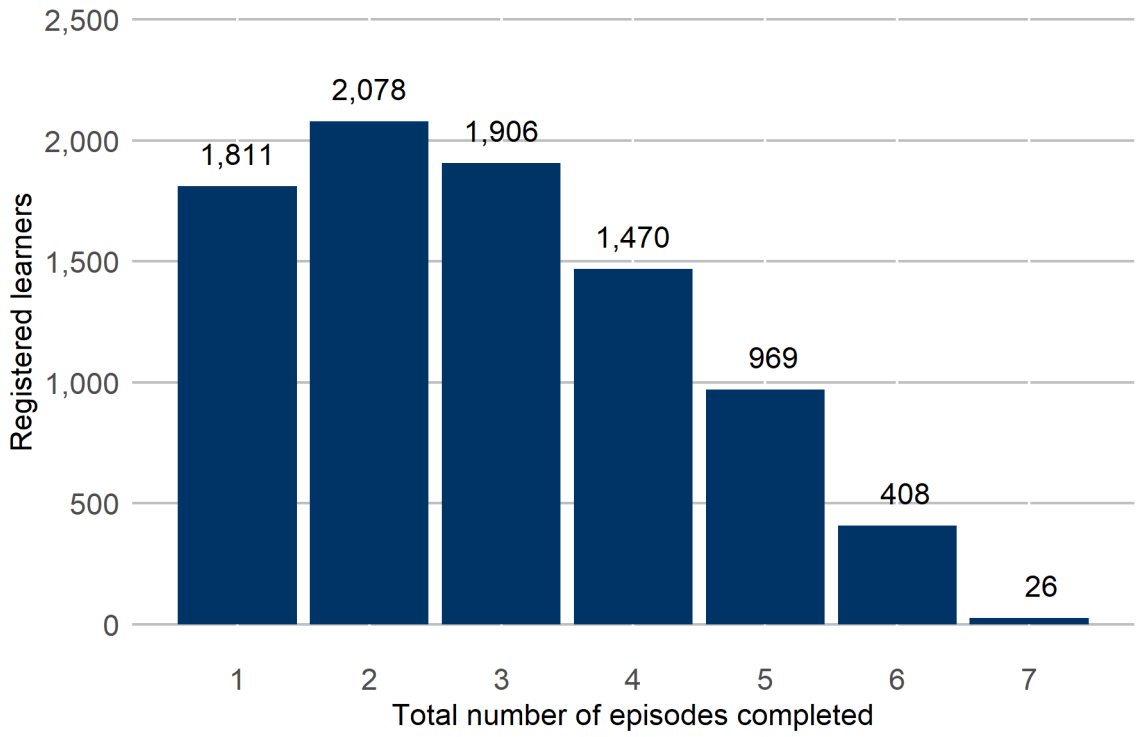
Registration data showed that 8,668 out of 22,778 registered learners (38%) completed at least one module, while 434 out of 22,778 (2%) completed at least six out of seven modules of content. 14,110 out of 22,778 registered students (62%) were not recorded as having engaged with any of the content of the Cyber Explorers platform. The reasons for this are not fully understood. Feedback suggests that some students may be sharing terminals with other students in some classrooms so that only one student in a group is recorded by the system as having completed a module. Feedback from all stakeholders suggests that lower than expected engagement is largely related to the fact that the launch was in the second half of the school year, which meant that the programme ran at an inconvenient time, for example during busy exam periods and approaching the summer holidays. It is worth noting that an impact analysis would ideally assess the outcomes of those learners that have been fully engaged[8] with the platform, as they would be expected to show the most signs of impact caused by the programme.

[7] UK Cyber Cluster Collaboration (UKC3) supports cyber clusters to drive growth of the cyber sector within their nations and regions, encouraging greater collaboration across the UK's cyber ecosystem. https://www.ukc3.co.uk/

[8] By QA's definition, learners who have logged in and completed approximately 85% of the Cyber Explorers content (i.e., at least 6 modules) are defined as 'engaged'

However, as shown in the next sections, we lower the threshold of engagement to at least one module for the purposes of using a larger sample in our impact analysis.

Figure 2: Module completion among learners completing at least one module (38%, n=22,778)



Source: Ecorys analysis of QA data

User characteristics

While the demographic data collected at registration shows the profile of all learners registered by educators, the profile of learners who initially engaged with the Cyber Explorers platform and responded to the System Questions can be examined by assessing the demographics of those who reached that stage. The 5,244 respondents answering the System Questions form a sub-sample of the total 22,778 registered learners analysed in the previous section. This sub-sample refers to learners who answered the System Questions and engaged with the platform by completing at least one module out of 7[9]. The sub-sample was used throughout the rest of the analysis for this report and is therefore referred to as the "users" of the platform. Using this data allows us to examine the profile of those who are actively engaging with the platform, with this being important given that many of those who registered in the programme may not go on to use the platform.

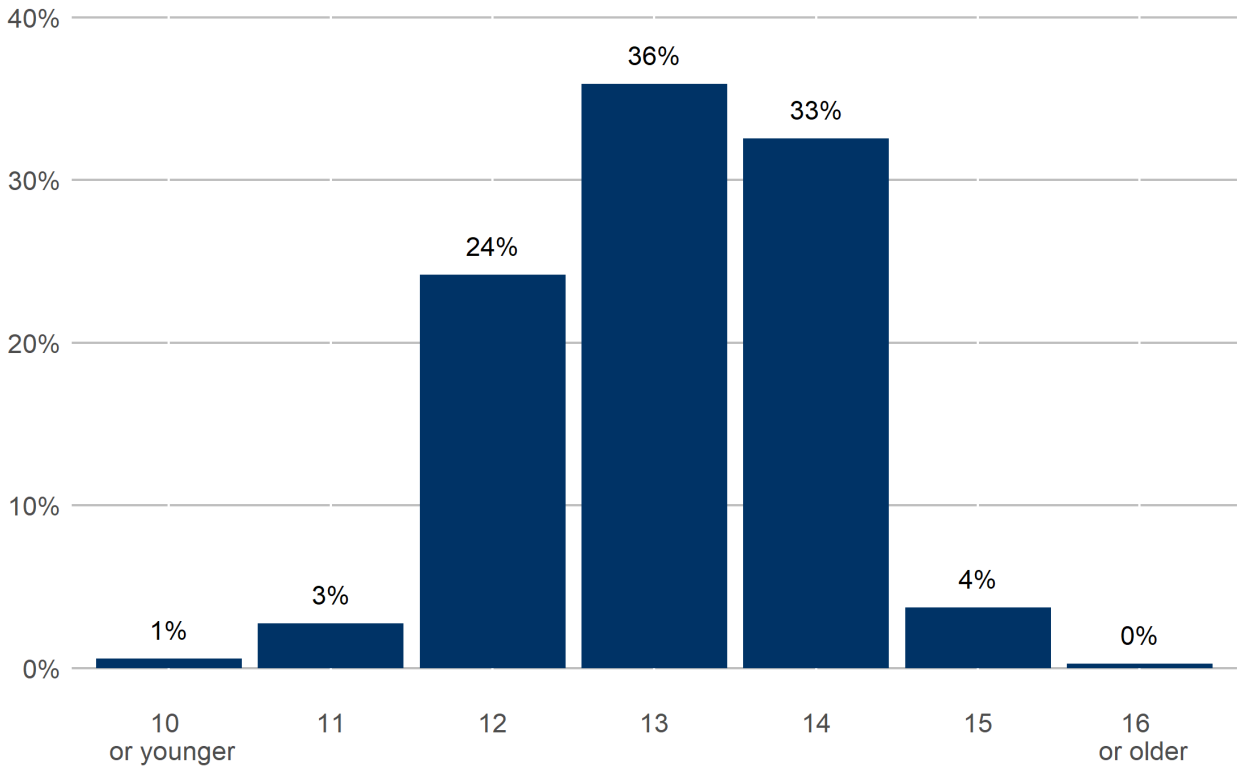
[9] Completion of at least 1 out of 7 modules refers to the general engagement of these learners regardless of when they answered the baseline System Questions. Most of these learners completed the System Questions and then went on to complete at least one module, although there might also be students that first completed 1 module and then went back to complete the baseline System Questions.

As with all registered learners, MI data was also collected for this sub-sample, which was used to construct a profile for these users. However, not all MI data was mandatory, resulting in different base sizes for some questions (e.g., not all participants have given consent to disclose their ethnicity).

The profile of Cyber Explorers users is shown below:

- Out of the 5,145 participants with age data, most were 13-14 (69%), with a smaller proportion being 12 years olds (24%), and only 3% being 11. This suggests participants tended to be on the older side of the target age groups (11-14 years old).

Figure 3: Age distribution of Cyber Explorers participants (n=5,145)



Source: Ecorys analysis of QA data

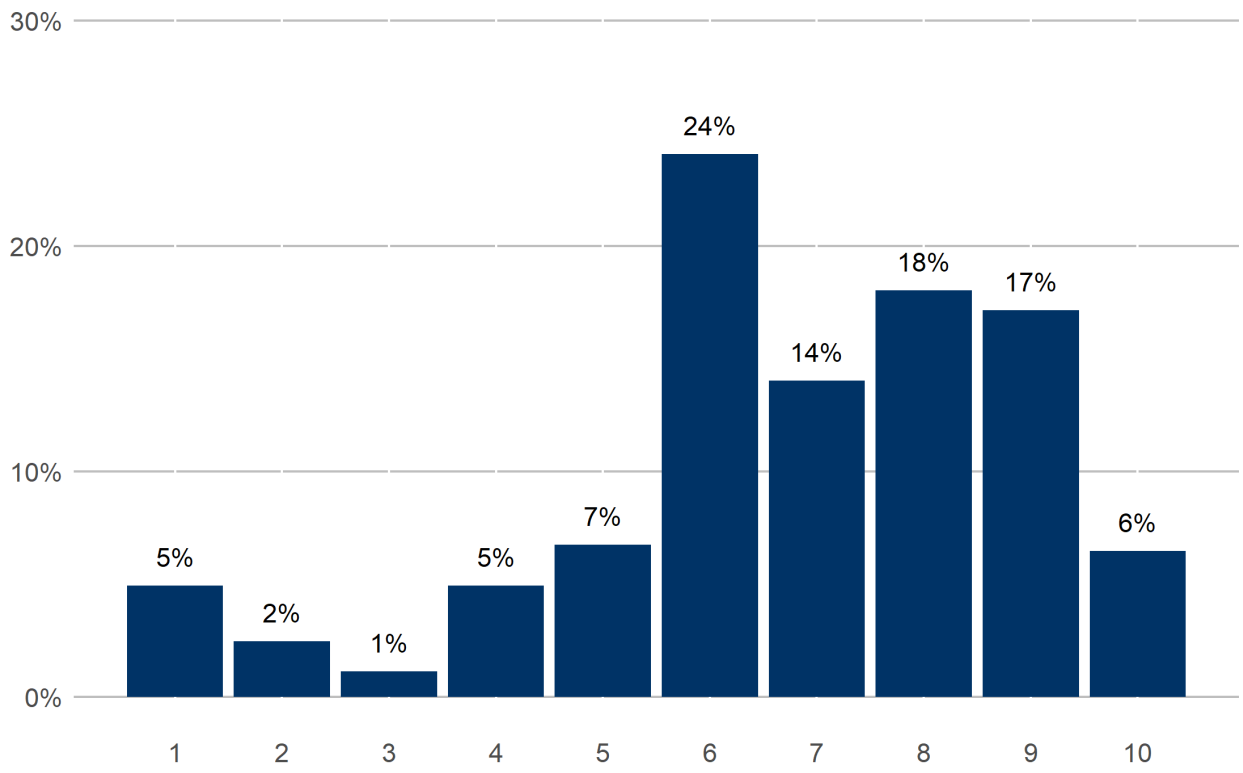
- The gender distribution among the 4,167 users with gender data was almost equal, as 50% of users were male and 49% female, while less than 1% selected “other”.
- Most of the 1,930 users with ethnic status data came from white ethnic backgrounds (76%), with 24% from ethnic minority backgrounds. This compares to 29% of Cyber Discovery participants being from ethnic minority backgrounds, although this is higher due to the higher age range for Cyber Discovery (data

suggesting the proportion of ethnic minority participants taking Computer Science being higher as students age).[10]

- The majority of users (91%) came from non-pilot areas, while 9% came from pilot areas (n=5,243).
- The majority of users attended state schools (82%), with 18% from non-state schools (n=4,512). In comparison, in the final year of Cyber Discovery, 74% of schools (not users) were state schools and 12% were independent, with no information on school type available for the remaining 14%. This suggests there may be little difference in the balance of state/independent school participation across the two programmes.
- The proportion of users from the three most deprived deciles was almost 9% while the proportion of those from the 5 most deprived deciles was 20%. This suggests that those in the more deprived deciles have not moved through from registering to using the platform at the same rate as those in less deprived deciles. This may be due to block-registering being more likely to occur in these areas, or due to genuine differences in participation patterns.

[10] In comparison, 22% of students taking Computer Science GCSE were ethnic minority students [The Roehampton Annual Computing Education Report: Data from 2017]

Figure 4: Cyber Explorers participants by Indices of multiple deprivation (IMD) deciles (1=most deprived, 10=least deprived, n=5,243)



Source: Ecorys analysis of QA data

A major theme from educator interviews was that the platform was felt to be suitable to a diverse range of students, including in terms of gender, ability level, and subject area. A minor theme from learners was that more could be done to make the content accessible for those who had dyslexia, for example reducing the amount of text and using different colours.

System Questions (SQ) respondents who engaged with the platform ("users") were also compared against other engaged registered users (i.e., those who did not answer any of the System Questions but engaged with Cyber Explorers). This comparison was made to assess whether the sample of System Questions respondents can be considered representative of Cyber Explorers participants. The two groups were tested against a set of demographic characteristics, as shown in the table below.

Table 5: System Question respondents vs. registered learners

Characteristics		SQ Engaged respondents		Registered Engaged learners	
		Freq.	Percentage	Freq.	Percentage
Gender	Female	2061	49%	1234	48%
	Male	2091	50%	1323	52%
Ethnicity	Non-white	461	24%	284	25%
	White	1469	76%	857	75%
Pilot	Non-pilot area	4783	91%	2913	85%
	Pilot area	460	9%	511	15%
Type of School	Non-state school	815	18%	509	18%
	State school	3697	82%	2366	82%
Deprivation deciles	IMD3	447	9%	409	12%
	IMD5	1060	20%	737	22%

Source: Ecorys analysis of QA data

Overall, SQ respondents who engaged are representative of Cyber Explorers participants in terms of age[11], gender distribution, ethnicity, type of school, and deprivation deciles (IMD3 and IMD5), as there were no meaningful differences[12] between groups in those characteristics. The two samples were not balanced only in terms of pilot areas, as relatively more users (91%) from non-pilot areas answered the System Questions compared to registered engaged learners (85%). The higher proportion from non-pilot areas among users than those registered tentatively suggests that non-pilot participants were sustained after initial engagement at higher levels than pilot participants. Overall, we deem that the sample of SQ engaged respondents is representative of Cyber Explorers participants as differences between groups are minor and can potentially be weighted in future analysis.

A sub-sample of engaged learners responding to the SQs before completing the content (n=5,107) was also used to compare against our counterfactual survey sample (n=1,015 of matched pre-post respondents). The characteristics, as well as baseline SQ levels of the two samples were compared to assess whether the two groups are comparable and if they can be used in impact analysis. Our analysis showed that the two samples are different across all characteristics and baseline outcome levels, except gender distribution which is balanced across the two samples. This suggests that any future impact analysis should consider weighting or matching[13] methods to improve comparisons and subsequently estimates of impact.

[11] Age is not shown in this table as we compared means across groups instead of percentages or frequencies. Both SQ engaged users and engaged registered learners were on average 13 years old.
[12] Standardised mean differences above 0.05. All 'balance checks' in our analysis assess whether samples are different based on this criterion.
[13] For example, techniques such as Propensity Score Matching (PSM) or Inverse Probability Weighting (IPW) are able to control for these differences.

In this report, as shown in the above diagram, the impact analysis was based on a sub-sample of SQ engaged users (n=23), which poses two separate challenges:

1. The sample might not be representative of Cyber Explorers participants as a whole (for example it does not contain any participants from pilot areas)
2. The sample might not be comparable to the counterfactual survey sample (as the sample of 5,107 SQ respondents is different to the counterfactual sample)

Differences between groups can usually be controlled for by using weights, however the small sample does not allow us to do so at this stage. Weights applied to a very small sample size can lead to loss in accuracy of results, for example running the risk that a weight is applied on an outlier observation. The sample was also missing certain information, for example there were no participants from pilot areas (all 23 respondents were from non-pilot areas), thus preventing us from applying weights to control for differences in responses among pilot and non-pilot participants. Impact findings below should therefore be interpreted with considerable caution, while further analysis with potentially bigger samples in the future is recommended.

Educator participation

This section discusses how and why educators became involved in the Cyber Explorers programme and plans for delivering it in and outside the classroom. It draws on the educator survey and interviews.

How educators heard about the programme

A major theme from interviews with educators was that they had discovered Cyber Explorers through their involvement with other CyberFirst programmes. For example, some educators reported receiving emails from CyberFirst that promoted Cyber Explorers, with one interviewee mentioning that learners had tried out Cyber Explorers at a CyberFirst Girls Development Day. A minor theme was seeing Cyber Explorers publicised on social media channels and online forums, such as professional Facebook groups.

Reasons for participation

A major theme from interviews with educators was that perceived benefits of participating in Cyber Explorers tended to focus on outcomes for learners, rather than outcomes for educators or the wider school. This was viewed positively by educators who were looking for extra-curricular opportunities for their students. However, a minority also mentioned that they were keen to see if the programme would improve their own knowledge of career opportunities and pathways. One educator also noted that they were interested to see if the programme would help the school teach cyber security in a more engaging and fuller way, as cyber security is not currently a large part of the Key Stage 3 curriculum.

Educators identified a range of factors that influenced their decision to take part in Cyber Explorers, namely, to improve pupils' knowledge of career opportunities in cyber security and computing; and to better inform their students about careers when making GCSE or equivalent choices. Specific reasons included overcoming stereotypes of the sectors associated with cyber security, particularly with a view to inspiring more female learners to continue pursuing computer science at GCSE level and beyond.

> "[The sectors] have been viewed as geeky, and there are still a lot of pupils who think it's massively geeky. They view it as someone sat in front of a computer screen for hours on end; basically, locked away from everybody else. It's about us trying to change that mindset." *Educator*

Another major theme was that regardless of career aspirations, educators were keen that all learners had a basic awareness of cyber security. Educators viewed this as essential for all jobs and for pupils' own personal safety. Interviewees highlighted wanting to ensure all students had a clear understanding of the importance of having a secure password, and awareness of cyber threats such as phishing schemes.

Some educators had taken part in other CyberFirst programmes, such as the Girls Competition and Cyber Discovery, and seen benefits for their learners so they felt confident the programme would be of a high quality and useful for their learners. A minor theme was that educators who had run Cyber Discovery noted they were looking for something to fill the gap since this programme had ended. A major theme was that educators felt confident in the programme as it was backed by the government.

A minority of educators mentioned participating in Cyber Explorers as it linked to other school activities that they were delivering at the time. For example, one school was running an Internet Safety Week, and Cyber Explorers seemed a good activity to include as part of this, while another school linked the programme with their Forensic Science Day.

Delivery approach and links to the curriculum

Most educators (75%) who responded to the educator survey felt there was at least some alignment between Cyber Explorers learning themes with their existing curriculum learning objectives, with 8% of them saying the alignment was strong, although more than a fifth (22%) were not sure (n=78). More than half of educators responded that they intend to use the Cyber Explorers website to supplement existing lessons on cyber security, while a fifth (20%) said they planned to use it as part of an extra-curricular IT club or similar activities (n=65). Educators reported overall high levels of confidence in teaching cyber security, as 58% said they felt "somewhat confident" and 38% said they felt "extremely confident" in teaching these subjects (n=69). This could reflect the role of educators who participated in the survey, as most educators responding to the baseline survey were IT/Computing/Digital teachers (81%), with just a minority being School leaders (9%), Careers lead or similar (3%) and other (8%) (n=78).

A major theme from interviews with educators and the delivery provider team was that educators used, or said they were planning to use, Cyber Explorers in a number of ways depending on how they saw the programme fitting with the curriculum and other timetabled commitments. A major theme was educators using, or planning to use, Cyber Explorers in the classroom as part of computing or ICT lessons. Minor themes included using the programme for homework tasks or as part of an extra-curricular computing club or similar. Feedback from the delivery provider and delivery partners suggests that computer science teachers and heads of department were the most responsive groups to promotional activity, compared to careers departments, head teachers and teachers from other subject areas. As a result, they reported that most recruitment activity was targeted at teaching staff in computing departments.

Delivery partners, policy stakeholders and educators suggested that a curriculum map would be a useful additional resource for educators to clearly map all the programme's content to the curriculum. There were mixed views presented on the extent to which the programme should introduce more links to the curriculum. A major theme from educators and learners was that learners enjoyed exploring content that goes beyond what they cover in lessons, and this was seen as an enabler to engaging learners in topics relating to cyber security. A minor theme was that not all schools offer computer science at GCSE or equivalent level, which can be a barrier to justifying time in the curriculum for content relating to computing and cyber security. It is therefore recommended that curriculum mapping should include links to wider subject areas, as well as computing subjects.

Industry partner participation

All seven industry interviews were conducted with industry partners attending a careers fair in one of the pilot areas, having been invited by the delivery partner in that area.

A major theme across interviews was that industry partners saw their involvement in terms of benefits for their organisation, including an opportunity to raise awareness of future recruitment opportunities at their company, to promote the company or brand in general, and to engage with young people to inform future training programmes. For example, one partner is exploring offering apprenticeships in cyber security and artificial intelligence, so they were keen to conduct market research with learners to understand which areas they are interested in pursuing in future.

Industry partners highlighted the value of providing positive role models whom young people could relate to, and the importance of reaching learners at a young enough age to inform their subject and ultimately career choices when they are older. Interviewees who had taken part in a panel discussion said that the discussion was particularly useful as it allowed them to talk about their role in more detail and answer questions from the audience.

Partners made several suggestions on how to improve future events. They generally wanted more time to interact and have conversations with learners than was possible on the day. The event featured a competition for learners involving collecting stars from each stallholder – partners recognised that this made sure learners visited each stall but felt it did not always allow for meaningful interactions as learners were concentrating on collecting stars rather than engaging in discussion. One partner suggested that future events could have a stronger focus on practical steps for learners interested in learning more or pursuing a career in tech, presenting possible job roles relating to different interests.

Outcomes and impact

Summary

- Survey data suggested that there are indications that the programme has increased learners' understanding, knowledge and skills relating to cyber security. Learners found the content interesting and noted that they enjoyed learning about topics beyond what they would cover in lessons.
- It was not possible to detect the impact on learners' interest in cyber security as a study subject or as a career. This may be due to small sample sizes and low levels of engagement with the content.
- Qualitative feedback suggested that some learners had developed a better understanding of how cyber security related to a range of job roles, and some expressed a new interest in pursuing this further when they were older.

Recommendations to improve data collection

The following recommendations are made to improve ongoing data collection to assess outcomes in the short and longer term:

- Further data validation on learner characteristics to attain more complete data
- Implement measures to ensure learners complete data collection exercises in the correct order and at the appropriate time

Recommendations to improve engagement

The following recommendations were made to increase overall engagement:

- Review content to ensure it is suitable for older age groups
- Introduce further curriculum mapping to wider subject areas
- Introduce more hands-on elements, such as quizzes and games
- Offer incremental increases in difficulty
- Further use of inspiration role models from industry to bring content to life
- Introduce an improved dashboard functionality for educators to monitor learners' progress

This section covers views on the platform and model; learners' cyber security interest, skills and knowledge; likelihood of pursuing further qualifications in computing or digital skills; and perceptions of cyber security careers. This section draws on the learner survey, System Questions, learner feedback and educator interviews. The quantitative analysis includes overall results based on three samples:

i) All respondents answering the pre–System Questions and engaging with the platform (n=5,107), and;

ii) A sub-sample of users responding to both pre and post System Questions as well as completing at least one out of 7 modules (n=23)

iii) All respondents of the learner survey (n=138)

A sub-group analysis was also conducted where relevant to compare baseline scores across a selection of characteristics/sub-groups. The analysis compared mean scores across all sub-groups and tested the statistical significance of their differences. Results at this stage should however be interpreted with caution, as they focus on the baseline responses of participants. Due to the lack of responses in post System Questions, there is no data to run impact analysis on a pre-post matched sample, and therefore assess potential differences in impact among sub-groups (for example, whether impact was more significant for female participants compared to male participants). This analysis is therefore aiming to help us understand how different sub-groups answered the System Questions before they engaged with Cyber Explorers, and to inform any potential future analysis or future programmes.

Functionality and content

Generally, learner feedback from the online feedback form and case study visits suggests that learners liked the interactive nature of the platform and found the content enjoyable. A major theme was the usefulness of integrating videos and activities into their learning. They discussed how the videos were enjoyable compared to the usual format of learning they received in lessons. It was noted that including videos alongside tasks made them easier to understand and to complete. A few said this interactive approach improved their focus on the activities they were being asked to do. However, not all said they engaged with the programme, with some saying that it was easy to skip or not progress during the lesson without consequences.

> “I found the learning enjoyable because all the activities were based around fun things and made it rewarding to have the videos to watch at the start and the end.” *Learner*

A major theme from learners was that they would like to see more interactive challenges and games that would enable them to test their knowledge and skills in a gamified environment. In addition, it was suggested that the programme was text-heavy and would benefit from more diverse ways of presenting information. Some learners said this could prevent the programme from becoming repetitive and discourage learners from skipping ahead without fully engaging with the content. Educators noted that quizzes could provide incremental wins, helping with learner engagement.

A minor theme from learner feedback, and a major theme from interviews with educators, was the suggestion for additional challenges to introduce higher levels of difficulty. This

links to feedback provided in the student registration section of this report regarding perceptions of the programme being more suitable for younger students, as some educators noted that the level of challenge suited 11 and 12 year olds but was too easy for older students.

A major theme from learner and educator feedback was that they would like to see improved mechanisms for tracking learners' progress, and a reward system for completing content. Interviews highlighted that educators would like to see a more user-friendly dashboard that allows them to easily and quickly see how far along the course learners have progressed and what content they are currently looking at. One educator suggested time stamps showing when each learner completed an episode would be useful. Similarly, educators interviewed noted that including quizzes at the end of each episode and allowing educators to see learners' scores in these quizzes, would help them in gauging learners' understanding.

Some learners mentioned specific elements of Cyber Explorers that they enjoyed learning more about and pursuing. For example, the opportunity to understand more about Python and engage with it was described as fun and enjoyable. Another student enjoyed learning how to encrypt and de-encrypt data to keep it safer, whilst other students discussed enjoying learning about programming and its role in the technology they use regularly.

> "I think it [the platform] is good for looking at programming and it is quite interesting seeing how things work behind all these different tech things." *Learner*

> "My favourite part of the Cyber Explorers programme was learning how to encrypt and decrypt data to keep your information safe." *Learner*

A major theme was that learners reported having technical issues relating to the registration process and accessing the platform. They said that issues around creating accounts, logging on, and difficulty in remembering suitably complex passwords made accessing Cyber Explorers challenging. A minor theme was the slowness of the platform. It lagged during some activities and was reported to have crashed for others, impeding their engagement.

> "I really like the idea of this but I still think there can be improvements, such as making the site easier to log into and less laggy." *Learner*

Learners were asked to report on roughly how many hours they had spent on the Cyber Explorers website at the time of completing the baseline learner survey (i.e., before they fully engage with the content). Overall, learners had spent 1.5 hours on average, as a

third of respondents had not spent any time at all (33%), and almost half of them (47%) spent between 1 and 2 hours (n=138).

The learner post survey included a set of questions around the usability of the platform, for example how easy it is to navigate through the content and complete the available course. However due to the lack of post data from the learner survey, we are not able to assess this.

Cyber security

Cyber understanding

The impact analysis showed **early indications of an increase in cyber security understanding among participants**, as engaged[14] learners showed a higher average score in understanding by 0.4[15] compared to the counterfactual sample (i.e., those not participating in Cyber Explorers). However, completing an additional module did not have a significant effect in increasing cyber security understanding among learners. As there was a statistically significant difference on average (i.e., for different levels of engagement) but not for one additional module, this could suggest that learners would have to complete multiple modules for that impact to materialise. For example, students that complete three modules might experience a change in their cyber understanding, while students that complete module 6 after module 5 might not see a significant change. It is also possible that such changes (i.e., completing one additional module) are too marginal to detect due to the small sample size used in this analysis.

As mentioned above, these results should be interpreted with caution due to the small sample (n=23), and potentially tested further in the future with a bigger sample. In the rest of this section, we present baseline results (i.e., System Questions responses before completing Cyber Explorers content, n=5,107) regarding cyber-related understanding. This is aimed to help us understand more about the profile of Cyber Explorers participants, their initial levels of understanding, and to inform the potential future phases of the programme.

The following table shows baseline results in cyber-related understanding among Cyber Explorers learners.

[14] Engagement here is defined as having completed at least one module. This was done so that the biggest possible sample is used, as there was a very limited sample completing at least 6 modules (by the original QA definition of engagement). This means that engaged learners in this analysis have completed different numbers of modules (some have completed one, others 7), thus the impact detected should be interpreted as the 'on average' difference in the outcomes of those learners.

[15] Cyber security understanding is measured as a score from 1 to 5, with 1 being "almost nothing" and 5 being "very good understanding". Impact is measured as the mean difference in scores between Cyber Explorers participants and non-participants, all other things being equal (see Annex One: Impact analysis for more details).

Table 6: Self-rating of cyber security understanding among Cyber Explorers participants

"How would you rate your understanding of cyber security?" (Mean score=3.2/5, n=5,107)	Freq.	Percentage
I believe I have a very good understanding of cyber security, why I need it and how it applies to myself and others	570	11%
I believe I have a good understanding of cyber security, but I could learn more	1650	32%
I believe I have a general understanding of cyber security, but there's still a lot I don't know	1649	32%
I believe I only have a limited knowledge of cyber security	774	15%
I believe I know almost nothing about cyber security	464	9%

Source: Ecorys analysis of QA data

A small proportion of respondents rated their cyber security understanding at the top (11%) or bottom (9%) levels. In total, 64% of respondents felt that they have good understanding of cyber security, but there is still a lot they do not know/they would like to know more, suggesting a reasonable level of current understanding, with 15% saying they had a limited knowledge.

The following table shows the results of the sub-group analysis on baseline levels of understanding of cyber security:

Table 7: Cyber security understanding: sub-group analysis (n=5,107)

Characteristic	Sub-group	Mean	n	Difference	p-value	Statistically significant
Pilot area	Non-pilot	3.2	4,662	0.2	0.001	Yes
	Pilot	3.0	444			
Gender	Female	3.1	2,004	-0.2	0.000	Yes
	Male	3.3	2,038			
State school	Non-state school	3.3	788	0.0	0.307	No
	State school	3.2	3,597			
Deprivation deciles	IMD 4-10	3.2	4,674	0.0	0.772	No
	IMD Top 3	3.2	432			
	IMD 6-10	3.2	4077	0.1	0.111	No
	IMD Top 5	3.2	1029			
Ethnicity	Ethnic minorities	3.2	443	0.0	0.736	No
	White	3.2	1435			

Source: Ecorys analysis of QA data

Note: Differences between means are statistically significant at the 5% level, if their corresponding p-value is below 0.05

Sub-group analysis shows there were no significant differences by deprivation decile, ethnicity, or state school, with significantly higher results for those from non-pilot areas and males than their counterparts. While differences for these groups are statistically significant, they are relatively small and unlikely to be meaningful from a programme development perspective.

A major theme identified from learner feedback was increased awareness of the dangers of hacking and cyber-crime through the internet, key aspects of cyber security. Some learners said the programme helped them be more aware of what they were doing online and to avoid suspicious links or websites, in turn reducing their risks of viruses or dangers when using the internet. Examples of this included learning about two factor authentication, improving the quality of passwords and considering security when using social media. When asked what they enjoyed, one student said:

> "I found the games fun. The different types of viruses you could download (trojan horse, ransomware) hasn't helped me yet as I don't download things that often, but it probably will in the future." *Learner*

When asked how they thought Cyber Explorers may have helped them, a major theme was that the programme would change their future behaviour in terms of trusting reliable sources.

> "I think that all of them helped me to be safe on the internet. It helped me to not trust everything on the internet. I learnt to never click a link or trust a website." *Learner*

> "It helped me understand more about the dangers online and how it can affect my personal life. I learnt a lot about the safety and significance in keeping your details safe online." *Learner*

Beyond the personal cyber security skills, a further theme was that the programme had improved learners' understanding of cyber security as a concept and their interest in it. They described the benefits of the programme's *"fun," "enjoyable*" and "*engaging"* functionality as a mechanism that helped them pay more attention to learning about cyber security than they might have done in standard lesson format.

Cyber security knowledge

Learners were asked to report as part of the learner survey on whether they knew what cyber security meant and their knowledge around staying safe online, rating on a 0 to 10 scale (higher as more positive). Caution is required in interpreting data from the learner survey given the small base sizes involved (approximately n=138 across all survey responses), as a small size might not be representative of overall Cyber Explorers participants. In addition, the post-survey did not receive any responses from engaged[16] students, hence we report only on baseline figures (i.e., before they took part in the programme). This means that at this stage we cannot draw any inferences about potential changes in perceptions and knowledge caused by the programme.

[16] Engaged is defined as having completed at least 6 modules of content

This data showed that learners (n=138) felt they understood what cyber security meant, with the majority (88%) either saying they "definitely know what it means" (49%) or "probably know what it means (39%), suggesting confidence in a fundamental understanding of the subject, although a small minority lacked this basic knowledge. Similarly high scores were seen in terms of knowledge about staying safe online, as the majority of students (67%) rated their knowledge between 8 and 10 out of 10. A quarter (24%) of the 138 respondents to this question scored their understanding at 10 out of 10, while the overall average score was 8. Survey results suggest that participants at initial stages believe they have a good understanding of relevant issues.

Cyber-related skills

The impact analysis showed **early indications of an increase in cyber security skills among participants**, as engaged[17] learners showed a higher average score in understanding by 0.4[18] compared to the counterfactual sample (i.e., those not participating in Cyber Explorers)[19]. However, completing an additional module did not have a significant effect in increasing cyber security skills among learners. As there was a statistically significant difference on average but not for one additional module, this could suggest that learners would have to complete multiple modules for that impact to materialise.

As above, these results should be interpreted with caution due to the small sample (n=23), and potentially tested further in the future with a bigger sample. In the rest of this section, we present baseline results (i.e., System Questions responses before completing Cyber Explorers content, n=5,107) regarding cyber security skills. This is aimed to help us understand more about the profile of Cyber Explorers participants, their initial levels of self-perceived skills, and to inform the potential future phases of the programme.

[17] As above in sections covering the impact analysis, 'engaged' learners were those that completed at least one module.
[18] As above, cyber security skills are measured as a score from 1 to 5, with 1 being "any skills" and 5 being "expert skills". Impact is measured as the mean difference in scores between Cyber Explorers participants and non-participants, all other things being equal (see Annex One: Impact analysis for more details).
[19] The difference was statistically significant at the 5% level.

The following table shows baseline results in cyber security skills among Cyber Explorers learners:

Table 8: Self-rating of cyber skills among Cyber Explorers participants

"How would you rate your cyber security skills?" (Mean score=3.0, n=5,107)	Freq.	Percentage
I have expert cyber security skills which give me complete confidence to keep myself safe online	394	8%
My cyber security skills are sufficient to keep me safe, but I'd like to know more	1556	30%
I have some good cyber security skills but there is still a lot I am unsure of	1625	32%
I know a little about cyber security but struggle with applying it	940	18%
I don't feel as if I have any cyber security skills	592	12%

Source: Ecorys analysis of QA data

Relatively few rate their skills as ‘expert’ (8%) and a similarly small proportion feel they have no skills at all (12%). Most participants feel they have some level of skills but would like to know more (30%), there is a lot they are unsure of (32%) or they know a little but struggle with applying it (18%). This suggests a perceived need for improving cyber security skills among most participants, and the potential for Cyber Explorers to deliver change.

Data also suggests that learners may have a different perception of their skills than their teachers, although the low number of responses from the educator survey means results should be treated with considerable caution. Data from the educator survey shows that less than a third of educators (28%) felt that most of their learners (between half and all) have sufficient skills to remain safe online (n=71).

A potential reason for any low skills among learners is poor access to resources at home. Poor access appears to be an issue for a notable minority of learners, with 3% of educators stating that more than three-quarters of their students have difficulty completing digital tasks at home due to having no computer or suitable device, or no/poor internet connection, 10% around half, and 2% between a half and three quarters. Most teachers (54%) said less than a quarter had these issues and 13% said less than half, while 14% stated that none of their students were affected (n=63).

The following table shows the sub-group analysis for rating cyber security skills:

Table 9: Cyber skills: sub-group analysis (n=5,107)

Characteristic	Sub-group	Mean	n	Difference	p-value	Statistically significant
Pilot area	Non-pilot	3.1	4,662	0.3	0.000	Yes
	Pilot	2.8	444			
Gender	Female	2.9	2,004	-0.2	0.000	Yes
	Male	3.1	2,038			
State school	Non-state school	3.1	788	0.1	0.140	No
	State school	3.0	3,597			
Deprivation deciles	IMD 4-10	3.0	4,674	0.1	0.216	No
	IMD Top 3	3.0	432			
	IMD 6-10	3.1	4,077	0.1	0.179	No
	IMD Top 5	3.0	1,029			
Ethnicity	Ethnic minorities	3.0	443	0.0	0.919	No
	White	3.1	1,435			

Source: Ecorys analysis of QA data

Sub-group analysis on cyber security skills shows similar results to the sub-group analysis on self-rated understanding around cyber security. There were no significant differences in self-reported skills by deprivation decile, ethnicity, or state school, but significantly higher results for those from non-pilot areas and for males compared to their counterparts. Males reported relatively higher cyber security skills (3.1 compared to 2.9 for females), as well as those in non-pilot areas (3.1 compared to 2.8 for those in pilot areas). While this initially suggests important differences between these groups, the relative differences between the two groups in each case, and as above with cyber security understanding, are relatively minor.

Interest in cyber security

Learners were asked in the learner survey to rate their interest in cyber security on a scale of 0 to 10 (higher as more positive). As above, caution is required in interpreting data from the learner survey given the small base size (n=138) and the lack of post data to compare and identify potential changes due to participation in Cyber Explorers.

Participants reported an average interest in learning about cyber security (5.7 out of 10), with only 14% providing a score of 8 to 10. Combined with the other data, this suggests that learners felt they have a solid basic understanding and knowledge of cyber security, generally felt they have good skills, but do not have the same level of interest in learning about the subject.

Finally, the learner survey asked respondents two questions about their perceptions on gender in cyber/digital subjects and jobs: firstly, whether computing/digital subjects are viewed as more masculine or feminine; and secondly whether jobs in cyber security are

more suitable for men or women. Data from this survey showed that the majority of respondents viewed computing/digital subjects as neither masculine or feminine (60%, n=138), and viewed jobs in cyber security as equally suited to men and women (70%, n=138).

A quarter of respondents said that jobs in cyber security are more masculine (24%, n=138) while a sixth of respondents said that such jobs are more suited to men than women (17%, n=138). However only 1-2% of respondents felt that such jobs are slightly more feminine/more suited to women (n=138). It is generally positive that despite any views of masculinity/femininity, most respondents found that jobs are equally suited to both men and women, suggesting a perception that both men and women are capable to do such jobs. The fact that 17% of respondents felt that jobs in cyber security were more suited to men suggests however, that there is further room for development.

Cyber security careers

45% of respondents (n=138) said that they have thought a lot about their future jobs, with a further 41% reporting they have thought about this a little. While this suggests a reasonable level of consideration, this does not necessarily mean that relatively definitive choices have been made, and potentially just that certain broad options have been considered. However, it shows a general engagement, even at a relatively young age, with issues around career choice.

The following table shows results on the main outcome questions around cyber security careers. As previously, main outcome indicators from the learner survey are measured using a scale from 0 to 10, where 0 is “I know nothing” or “not at all interested”, and 10 is “I know a lot” or “extremely interested”.

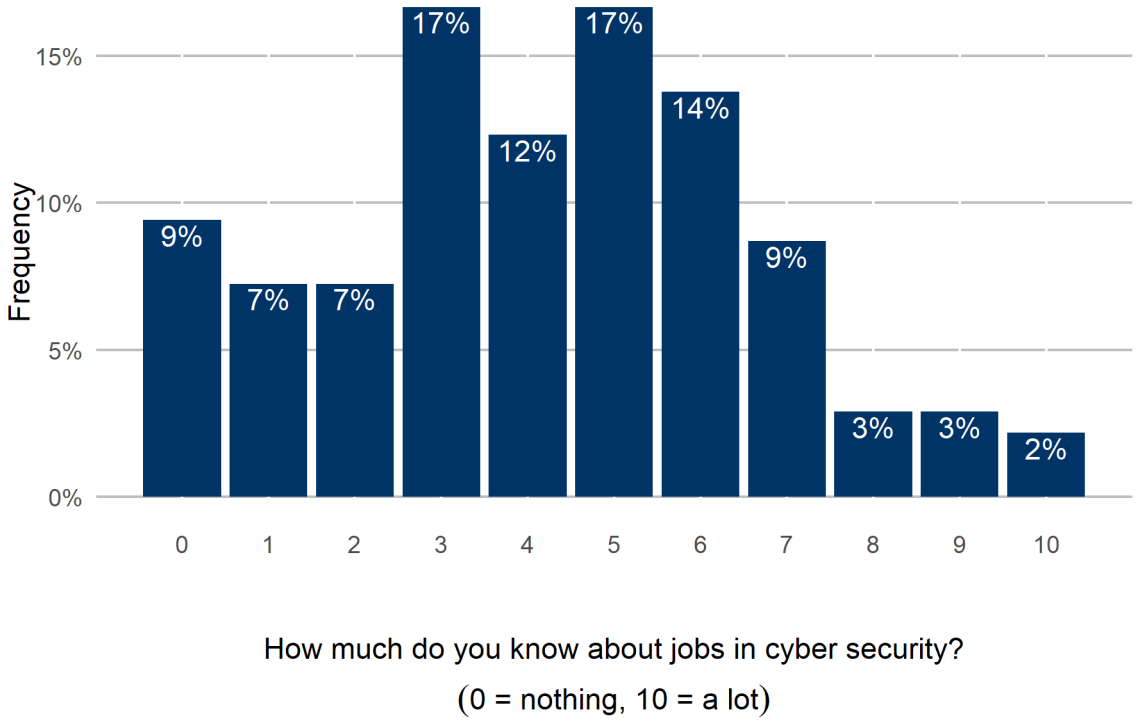
Table 10: Learner survey outcomes: learners’ scores on cyber security careers Main outcome indicators (scale 0-10)

Main outcome indicators (scale 0-10)	Mean	St. dev.	N
How much do you know about jobs in cyber security?	4.2	2.5	138
How interested are you in a job in cyber security?	4.1	3	138

Source: Ecorys analysis of QA data

Participants self-rated their knowledge about jobs in cyber security on average at 4.2 out of 10, although as the below graph shows this varied considerably across respondents. Most participants (59%) rated their knowledge between 3 and 6 out of 10, with 17% rating above 7 out of 10, and 24% rating 2 out of 10 and below. The sizeable minority giving a relatively low score suggests that successful cyber-related learning could improve basic levels of knowledge among young learners.

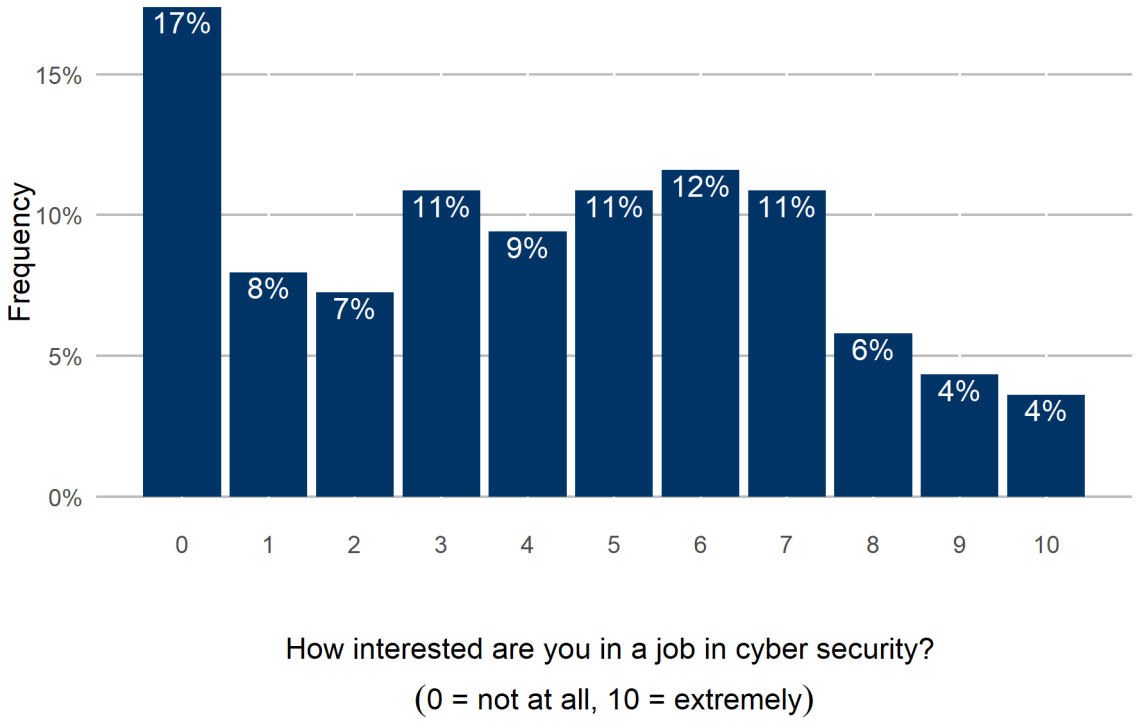
Figure 5: Self-reported knowledge about jobs in cyber security (n=138)



Source: Ecorys analysis of QA data

Learners rated their interest in jobs in cyber security at 4.1 out 10 (n=138), lower than their interest in cyber-related learning (5.7) but almost the same as their self-reported knowledge about jobs in cyber security (4.2). This indicates that a proportion of participants may have a general interest in the area, but are not necessarily interested in pursuing a career in cyber. Particularly notable is that only 14% of learners rated their interest in cyber jobs at between 8 and 10, while 17% of learners rated their interest at 0 out of 10. This could suggest that the cohort of learners with a very clear interest in cyber jobs at this stage is proportionally small, potentially unsurprising given the age of the young people and their prior involvement in cyber.

Figure 6: Interest in jobs in cyber security (n=138)



Source: Ecorys analysis of QA data

Learners also provided mixed responses when asked if a job in cyber security would be suitable for them. Almost a quarter of learners (23%) agreed that such jobs were for them and 8% strongly agreed, while 38% neither agreed nor disagreed and 11% were not sure, suggesting overall high levels of uncertainty (n=138). However, learners responded positively in terms of cyber security jobs being good for someone to have, as almost half responded “yes, probably” (46%) and 30% responded “yes, definitely” (n=138). This suggests a positive attitude towards cyber security jobs, as learners seem to agree that such jobs are suitable and good to have for others, regardless of their personal interest in them.

A major theme from qualitative learner feedback was that Cyber Explorers helped them to understand links between cyber security and potential career paths.

> “Cyber Explorers has made me more aware of the jobs in cyber security.” *Learner*

Some said that the programme helped them to understand the different types of job roles they could have within cyber security. They described the added value that understanding the risks of cyber security might have, even if they did not want to pursue a career in it directly. Examples of this included those wanting to be vets, working in labs, owning their own business and in hospitals.

> “I think cyber security would be useful for my desired career [a vet] and so I plan to take a crash course in computing after my A-levels.” *Learner*

> “It has made me more interested in learning more about computing and cyber security, so when I’m older and I want to start a business, I know how to secure it.” *Learner*

Some learners discussed Cyber Explorers prompting a further interest or *“rethinking*” of computing and IT, whereas some said directly that they thought it could be a career that would interest them in the future. A minor theme was that cyber security was not something they were interested in as a career choice but did see its added value in their own personal and professional lives regardless.

> “It has made it more interesting because it showed me how cyber security was in things that I didn’t realise.” *Learner*

> “It has helped me realise that whatever job I go into, I will need cyber security and it is important everywhere in life.” *Learner*

Others said that Cyber Explorers had led to them developing an interest in the potential for a career in cyber security, but they reflected that it would be useful to see more detailed information and real-life examples of different job roles. A major theme was that learners reflected positively on the different characters and stories they could follow, but some commented that they would like to see additional characters added to the platform, reflecting a wider range of job roles. It was suggested that having these characters exploring scenarios with them helped demystify cyber security for young people.

> “Helping the characters solve their problems made cyber security less intimidating and boring and more fun.” *Learner*

> “It would make it more interesting to add in real cases and make it more serious.” *Learner*

A theme from interviews with educators was that including video diaries or interviews with people who work in the cyber security sector would help further engage learners with the careers aspect of the programme. Educators noted that these would need to showcase the diversity of those working in the sector, both in terms of characteristics such as gender and ethnicity, and in terms of diversity in the skills needed to do these jobs. One educator noted that ‘big name’ organisations can add to the appeal and help young people envisage the types of jobs they might be able to do in the future.

> "Pupils are motivated by role models and seeing someone like them working in the sector – so for example, having a female who works in cyber security speaking to children about her work can be quite motivational [for female pupils]." *Educator*

A minor theme was that Cyber Explorers had shown learners that cyber security could be an opportunity for them to help people. Whether in their personal lives for friends and family or for future career prospects, learners described how they wanted to share the things they had learnt from the programme and use it to help others to stay safe from cyber security risks in future.

> "I want to tell others how to keep safe online and how to keep clean from any malware." *Learner*

Learner likelihood to choose cyber-related qualifications

The impact analysis showed **no indications of impact** in terms of willingness of Cyber Explorers participants to pursue further cyber qualifications (neither on average[20], nor caused by completing an additional module). As with the impact analysis on cyber-related understanding and skills (see above sections), these findings regarding cyber-related qualifications should also be read with caution due to the small sample of participants (n=23). Further analysis on potentially bigger samples is advised for any future phases of the programme and evaluation of the programme. As above, we also present the baseline findings of users around the likelihood of pursuing cyber qualifications, to inform our understanding and the future of Cyber Explorers.

The table below shows responses of participants on the likelihood to choose further cyber-related qualifications:

Table 11: Likelihood of choosing further cyber qualifications

"How likely are you to choose further qualifications in computing or digital skills subjects in your next stage of education?" (Mean score=2.8, n=5,107)	Freq.	Percentage
I almost certainly will choose to take a computing or digital qualification	548	11%
I am likely to choose to take a computing or digital qualification	706	14%
I am still undecided	1732	34%
I doubt I will choose to take any computing or digital qualifications	1272	25%
I almost certainly won't choose to take any computing or digital qualifications	849	17%

Source: Ecorys analysis of QA data

Participants generally reported mixed views about pursuing further cyber-related qualifications. Just a quarter (25%) were almost certainly (11%) or likely (14%) to choose a computing or digital qualification. A large proportion of participants was still undecided (34%), while the remaining 42% either doubted (25%) or almost certainly (17%) would not choose to take any cyber-related qualifications.

[20] As above sections regarding impact analysis, on average refers to 'engaged' learners, meaning those that completed at least one module.

It is worth noting that 41% of learners responding to the learner survey (n=138), reported that they had chosen to study IT, computing, or similar digital subjects at school, showing willingness to further their qualifications. Almost half of students (46%) reported that IT and similar subjects are compulsory at their school, while only a small minority of learners (5%) said they had chosen to drop these subjects (n=138). The majority of learners (83%) reported that their school offers IT, computing or a similar digital subject at GCSE, Standard Grade or equivalent (n=138).

Sub-group analysis was also conducted to compare likelihood of choosing cyber-related qualifications across multiple different characteristics and sub-groups.

Table 12: Likelihood of choosing further cyber-related qualifications: sub-group analysis (n=5,107)

Characteristic	Sub-group	Mean	N	Difference	p-value	Statistically significant
Pilot area	Non-pilot	2.8	4,662	-0.1	0.076	No
	Pilot	2.9	444			
Gender	Female	2.5	2,004	-0.5	0.000	Yes
	Male	3.1	2,038			
State school	Non-state school	2.8	788	0.0	0.982	No
	State school	2.8	3,597			
Deprivation deciles	IMD 4-10	2.8	4,674	-0.2	0.000	Yes
	IMD Top 3	3.0	432			
	IMD 6-10	2.8	4,077	0.0	0.695	No
	IMD Top 5	2.8	1,029			
Ethnicity	Ethnic minorities	3.0	443	0.3	0.000	Yes
	White	2.8	1,435			

Source: Ecorys analysis of QA data

Note: Differences between means are statistically significant at the 5% level, if their corresponding p-value is below 0.05

Sub-group analysis shows evidence that the likelihood to take cyber subjects is higher for males (3.1) compared to females (2.5), and higher for learners of ethnic minority backgrounds (3.0) compared to white ethnicities (2.8). The difference in scores between males and females is the highest among all sub-groups being compared, which suggests a particularly big gap in how males and females think about cyber security qualifications. This difference aligns with findings in the other System Questions above, as males also reported significantly higher levels of understanding and skills compared to females.

The likelihood of pursuing further cyber-related qualifications was also significantly higher for the top 3 most deprived deciles (3.0) compared to the rest (2.8), although there was no difference between the top 5 deciles and the rest. There was no statistically significant difference between students from state schools compared to non-state schools in terms of their likelihood of pursuing such subjects.

Anecdotal feedback from learners suggested that for a small number of learners, Cyber Explorers had made them further consider how cyber security related to their existing curriculum and subject interests such as graphic design or performance studies. Some students reported that participation in the programme had led to them deciding to pursue Computer Science or IT subjects in their GCSEs when they were not sure before or reaffirmed their interest in pursuing it if they were already on these programmes.

> "Cyber Explorers has made me more intrigued with learning computer science and I think it makes the lessons more enjoyable." *Learner*

Additional educator outcomes

Among educators interviewed, a strong theme was that learners appeared to be enjoying the programme. While some interviewees had only recently started using the programme and thus felt unable to comment further on outcomes, a major theme from educators who had progressed through several of the episodes was that they felt that the programme was having a positive effect on pupil awareness of cyber and computing careers. One educator noted that:

> "It has a lot more depth to it than the things we have used before…. compared to Cyber Discovery, this branched away from the stereotype of the hacker and typical IT group, [and] adds a bit more breadth to the idea that there could be an opportunity for jobs for everybody." *Educator*

Another educator emphasised the positive effect of the programme in terms of teaching pupils about areas of cyber security beyond coding.

> "There's a big focus on programming in the curriculum and in some other programmes, and while programming is obviously very important, [pupils] need to have knowledge of the other areas of cyber security." *Educator*

Educators, delivery partners and members of the delivery provider team identified a range of barriers to educators engaging fully with the programme. A major theme was that the delayed timelines proved to be challenging as many educators had already committed their timetable for the year, so although they were interested in registering and exploring the platform, they reported that they would not be able to implement the programme until the start of the new academic year.

Conclusions and recommendations

This section provides a short conclusion drawing together the main strands of evidence and a summary of the key recommendations for future phases of the programme.

22,778 learners registered for Cyber Explorers. This is below the initial KPI of 30,000 but exceeds the indicative target of 20,000 by the end of June which was set to accommodate the delayed timelines. The programme exceeded targets for female registrations (49% against a target of 25%), deprivation (21% of learners from a school in the three most deprived deciles against a target of 15%, although only 32% of learners were from a school in the five most deprived deciles against a target of 40%) and location (79% of learners from schools based outside of London and the South East against a target of 50%). Registrations were lower in pilot areas, with 89% of registrations coming from non-pilot areas.

Based on this evidence and feedback provided by delivery partners, the delivery provider and policy stakeholders, the following recommendations are made in terms of **registrations and promotion of the programme:**

- To overcome barriers to registration in pilot areas, it is recommended that in future phases, the delivery provider continues to engage regularly and directly with schools, gathering ongoing feedback from schools to address barriers such as a lack of time and resources.
- It is recommended that more specific guidance and contracts are issued to delivery partners to manage expectations of all parties, ensure that appropriate targets are set and consistent monitoring information is collected.
- It is recommended that the delivery provider and partners consider what more could be done to utilise existing networks, local contacts and knowledge to promote the programme in pilot areas, seeking their engagement as early as possible in the process.
- Briefing materials provided to delivery partners that suggest activities and resources to engage educators and students, and mechanisms put in place to share best practice in terms of activities that have worked well in different areas would be beneficial.
- The new self-registration option for learners planned by the delivery provider is a welcome mechanism to reduce burden on educators.

Analysis of engagement statistics suggests that actual engagement with the programme was low. Feedback suggests that this largely relates to condensed timelines which were a barrier to schools fitting new programmes in their timetable. It is expected that engagement will increase in the new academic year, so it is imperative that the programme is able to build on the enablers and barriers identified by key stakeholders to

increase the number of learners completing content. Specifically, the following recommendations are suggested to **improve engagement**:

- The programme funder (DCMS) and delivery provider (QA) should set out how engagement may be improved in future iterations, including how the majority of learners that have not completed a module might be further engaged with this or similar programmes.
- It is recommended that curriculum mapping should include links to wider subject areas, as well as computing subjects, given not all schools offer computer science at GCSE or equivalent.
- Updating content is recommended to meet the needs of learners, particularly older students.
- The use of inspirational role models from industry could be expanded to bring sessions to life and run hands-on sessions with students.

Due to small sample sizes, it has not been possible to fully explore the impact of the programme, but analysis of survey data provides indications that through participation in Cyber Explorers, learners have an increased understanding of cyber security and improved level of skills. Feedback from educators and learners suggests that participants enjoyed taking part in the programme and particularly responded well to the interactive elements, such as videos and challenges. Suggestions have been presented about how to further enhance the **user experience and ongoing data collection** including the following:

- It is recommended that the delivery provider considers how improved mechanisms for tracking learners' progress, and a reward system for completing content could be added. This may include more interactive challenges and games that would enable learners to test their knowledge and skills in a gamified environment.
- It is recommended that further data validation on learner ethnicity is undertaken by the delivery provider in future to attain more complete data.
- It is imperative that mechanisms are put in place to ensure learners complete data collection exercises in the correct order and at the appropriate time point to provide a larger and more robust sample for impact evaluation to be completed in future.

Annex one: Methodology

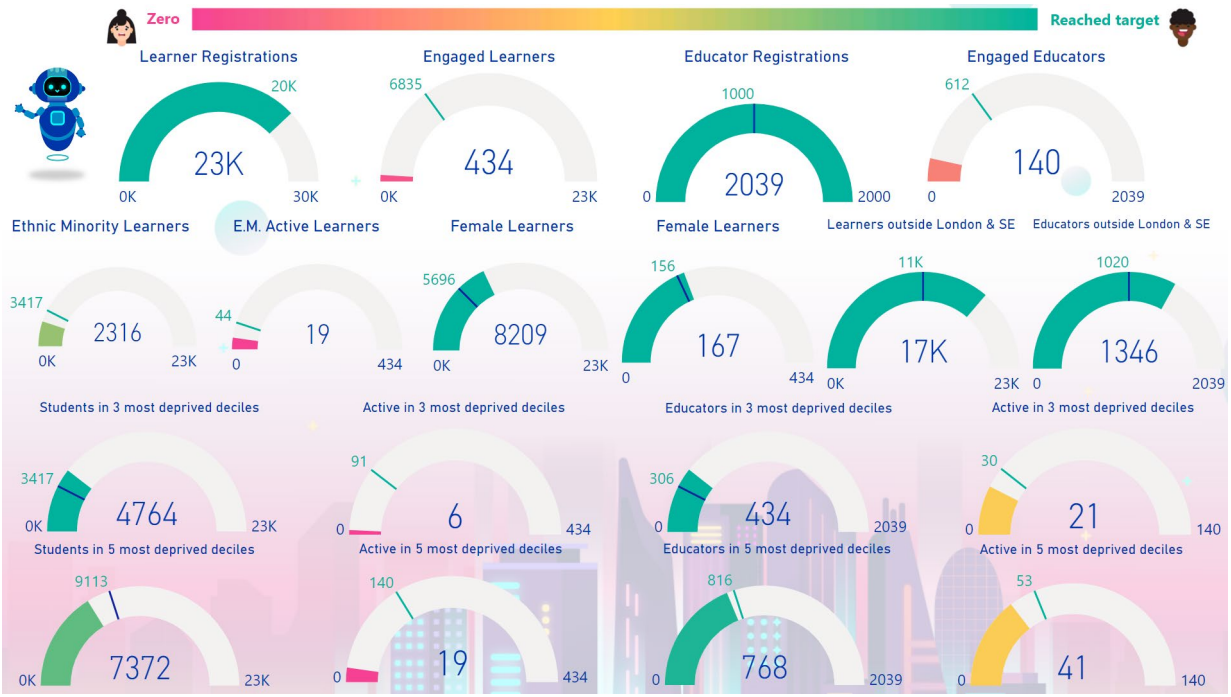
This annex provides a brief guide to the main elements of data collection for the Cyber Explorers evaluation, and which form the basis of this report.

Management Information

Management Information (MI) has been collected on an on-going basis since the programme started on 23 February 2022. The MI contains basic information provided by educators when they register for Cyber Explorers. This registration information includes basic information on their school, and demographic information for them and any young people that they also register (either by inputting individual details or bulk uploading spreadsheets with young people's details). In addition to showing the number and type of educators and young people registering, this data can also be combined with some other internal data to show similar figures for those who have engaged with the programme (defined as learners who have completed 85% of available content and educators who have signed up at least twenty learners).

It is not mandatory for educators to provide all MI, most notably demographic details for young people. As a result, there are gaps in the data, particularly for young people's ethnic status, with this not being completed for 76% of all young people who are registered.

MI data within this report is based on the MI data dashboard provided by QA to Ecorys on 20th July 2022. The core dashboard is shown below, and focuses on KPIs such as learner and education registrations, location, gender, and ethnic minority status.



Source: QA Management Information (provided for July 2022)

The data within the underlying MI and registration data includes the following core measures:

- Number of Learner Registrations
    - Age
    - Gender
    - Ethnicity
    - Location (including deprivation decile based on the Index of Multiple Deprivation data using the school postcode)
- Number of Educator Registrations
    - Location (including deprivation decile)
- Number of 'Active/Engaged' Learners and Educators
    - Markers for Learner Progress
- Number of Schools
    - State School/Private School
    - Location/Pilot Marker
- System Questions (segment by age, gender, ethnicity, decile, pilot, state school)
    - How likely are you to choose further qualifications in computing or digital skills subject in the next stage of education?
    - How would you rate your cyber security skills?
    - How would you rate your understanding of cyber security?

Management Information (MI) analysis

The MI data is examined in the report in two separate ways to allow us to examine whether the profile of participants changes through their participation in the programme. answer different specific questions. This includes:

- Analysing the profile of those who register, namely the full MI sample of all 2,039 educators and 22,778 learners registered
- Analysing the profile of learners who reached the initial System Questions to be completed once learners logged on to the system (see System Questions section in this annex). This analysis includes 5,611 learners (5,244 of which went on to engage with the platform by completing at least 1 module).

As educators may have registered young people who have not yet (and may not at all) log on to the platform, comparing the profile of learners who are registered with those who reach the initial System Questions allows us to assess participant characteristics in more detail.

Educator survey

The educator baseline survey is an approximately 10-minute online survey. The survey has been distributed to 1,304 registered educators who have given consent and are involved in Cyber Explorers activities (as of 21 July 2022). The survey is automatically sent to educators by QA as soon as they register and give consent. The survey was launched alongside the programme launch on 23 February 2022. The survey contains a variety of questions, primarily asking educators about their use of supporting materials and the extent to which these were helpful, educators' plans on using CE, educators' perceptions of their learners' skills and knowledge on cyber security, alignment with current curriculums, and confidence in teaching cyber-related subjects. Not all questions were mandatory, resulting in different levels of completion for different surveys. A follow-up survey was also sent from 11 of July to a total of 96 educators.

Educator survey analysis

As of 22 of July 2022 there have been 78 completed responses (6% response rate based on 1,304 registered educators who gave consent at that point) on the baseline survey. Most questions (marketing and supporting materials, confidence in teaching, perception on learners' skills and capacity on cyber security, etc.) were asked to all types of educators (i.e., career leads, school leaders/senior leadership, other subject educators), although it is worth noting that most of the educators responding to the survey were IT/Computing/Digital educators (n=63, 81% of total).

All baseline educator survey results are based on a relatively small sample (a maximum of 78 responses), although there were more than 2,000 educators registered with Cyber Explorers. This means that the sample of educators in this survey might not be representative of all educators engaging with Cyber Explorers. In addition, not all survey questions were mandatory, hence why available base sizes might differ. Due to the low sample size and response rate, findings from the educator survey are to be interpreted with considerable caution.

Two separate educator follow-up surveys were also sent, one for engaged educators (i.e., those who have registered 20 or more learners), and one for unengaged educators (i.e., registering less than 20 learners). The two surveys had similar questions regarding educator characteristics, views about Cyber Explorers and broader questions about cyber security, as well as relevant questions on engagement. The surveys had an equally low response rate (7%), which resulted in a total of 11 responses (8 engaged, 3 unengaged). This means that it was not possible to conduct a pre-post analysis on matched respondents, as the sample size was too small to detect any meaningful changes on educators' perceptions and attitudes towards cyber skills and cyber security (this would be based on a maximum of 8 matched engaged educators, which would not be sufficient).

System Questions

As part of the Cyber Explorers training programme, participants are encouraged to respond to a short set of “System Questions” embedded in the platform system. The initial questions were aimed to be completed when learners created an account, logged in, watched an introductory video and then clicked a button to provide details. This is an optional set of questions, which approximately 59% of participants responded to. These questions are mainly completed just before learners take part in the main body of Cyber Explorers, although it is possible for learners to start the programme and revisit the System Questions when they have completed some content. The three initial questions ask participants to respond to questions using a Likert scale from 1 to 5:

- "How likely are you to choose further qualifications in computing or digital skills subjects in your next stage of education?" (1=very unlikely, 5=very likely)
- “How would you rate your cyber security skills?” (1=don’t have any, 5=expert skills)
- "How would you rate your understanding of cyber security?" (1=almost none, 5=very good)

The follow-up set of questions includes these three questions, and an additional question (not using a Likert scale) asking:

- “How much do you know about jobs in cyber security? (I don’t know much about jobs in cyber security, I know a little about jobs in cyber security, I know a fair amount about jobs in cyber security, I know a lot about jobs in cyber security, not sure)

System Questions analysis

As of 21 July 2022, there were 5,696 completed responses to the System Questions, representing an average 59% response rate. The sample was reduced to 5,611 unique responses after data quality control and data cleaning, for example removing duplicates in the data due to students answering questions both in English and Welsh.

The analysis in this report makes use of a sample of 5,244 responses, which were all students who responded to the baseline System Questions, and went on to complete at least 1 out of 8 modules in the platform. This sub-sample was selected as it was the most representative of Cyber Explorers participants as a whole. The baseline analysis on these questions includes calculating frequencies and percentages for each response option (e.g., “I have a good understanding of cyber security”), mean scores (out of 5), and sub-group analysis (i.e., how did different sub-groups such as males and females respond to the System Questions).

There were 87 responses on the follow-up System Questions, 68 of which were matched with baseline respondents (meaning that the rest 19 respondents only completed the

follow-up but not the baseline questions). Of the 68, only 23 were completed in the right order, meaning that these learners filled in the baseline questions, then engaged with the programme by completing at least 1 module, and then completed the follow-up questions. Using this sample allowed us to draw comparisons pre-post and against the counterfactual sample (see below), although results should be interpreted with considerable caution due to the small size.

Learner survey

The learner survey is a baseline and follow-up online survey distributed to Cyber Explorers learners by QA as soon as learners are registered by an educator. The survey is only sent to learners where full consent for participation has been provided both by learners and their parents/carers. The baseline survey lasts approximately 10 minutes and primarily covers key outcomes in terms of perceptions and attitudes about cyber security skills, knowledge, and interest in learning and cyber-related jobs. Learners were asked to answer these questions thinking about the time before they were involved in any activities in order to collect baseline results.

There are also two follow-up surveys for learners, one for engaged learners (i.e., those who have completed 85% or more of the content), and one for unengaged learners (i.e., those who have not completed 85% of the content). The two surveys had similar questions regarding participant characteristics, views and outcomes about Cyber Explorers and broader questions about cyber security, as well as relevant questions on engagement.

Learner Survey analysis

There were 146 responses in total (as of 21 July 2022). After our initial data cleaning and quality assurance processes, 6 responses were removed resulting in 138 total responses.

This achieved sample size to date has been significantly affected by a variety of factors outside our control, resulting in a low response rate of 3%, suggesting that the final sample may not necessarily be representative of Cyber Explorers participants. One of the possible explanations behind the low response rates on this survey is that educators do not appear to have consistently accessed or provided consent, meaning that only approximately 29% of learners can be contacted. This low sample size means results should be interpreted with caution, and also means that sub-group analysis was not possible.

The follow-up surveys also showed low response rates, as there were less than five students responding to the survey, both of which were unengaged. This meant that analysis of potential change before and after engagement with the programme was not possible. Therefore, we only report on baseline results of this survey in this report.

Counterfactual survey

The counterfactual survey is a baseline and follow-up survey being conducted with young people aged 11 to 14 across England, using a panel provider with access to a representative spread of young people. All young people contacted have consent in place to be contacted for research purposes. The baseline and follow-up surveys each last approximately ten minutes and cover experience of cyber security training, and ratings on key outcomes including cyber skills and knowledge, and employment and curriculum choices.

There are two follow-up surveys which were completed during June-July 2022, one of which was distributed approximately 1 month after the baseline counterfactual survey, and one 2 months after. The two research waves utilised the same questionnaire and aimed to capture the variance among Cyber Explorers participants in completing the course.

Counterfactual Survey analysis

There were 4,315 responses in total to the baseline survey with 2,014 completed surveys, achieving our target of 2,000. This means a response rate of 45.5% from all those sent the survey, and a completion rate of 46.7%. There were also 1,015 completed responses in total (581 in wave 1 and 434 in wave 2) to the follow-up surveys, achieving our target of 1,000. Basic quotas on regions have been met.

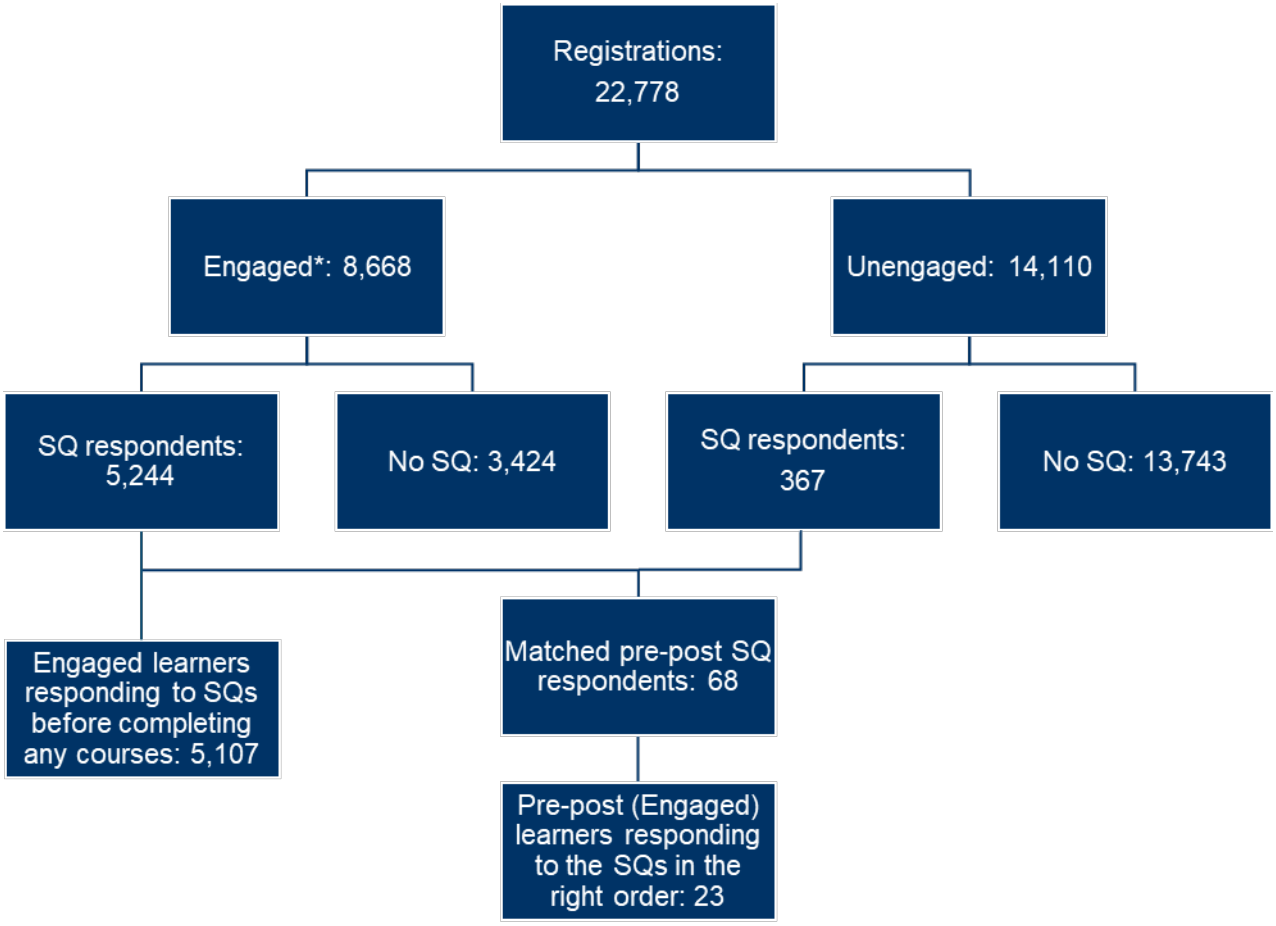
All 1,015 follow-up responses were successfully matched with the baseline, giving us a total pre-post sample of 1,015 responses. This sample was compared against the sample of 5,244 System Questions engaged respondents to assess whether the characteristics of the two groups are similar and inform future analysis and evaluation.

Impact analysis

The impact analysis entailed comparing the 23 System Questions engaged respondents against the counterfactual sample of 1,015 respondents, as well as before and after engagement with the Cyber Explorers programme.

The following diagram shows the sub-sample of 23 respondents was constructed and used in the impact analysis, starting from the total sample of registrations:

Figure 7: Samples for analysis (based on QA MI data)



Source: Ecorys analysis of QA data

**Engaged learners are defined as those completing at least 1 module*

The analysis focused on the three main System Questions around cyber security understanding, cyber skills, and likelihood of pursuing cyber-related qualifications, which were also asked in the counterfactual survey. All three indicators were measured as numeric scores of 1 to 5, with 1 being low understanding, skills, and likelihood, and 5 being high. Impact is defined as the mean difference in scores between the two groups (Cyber Explorers participants and non-participants), all other things being equal. For example, a positive and statistically significant difference of 0.4 in cyber understanding means that participants scored on average 0.4 points higher than non-participants (e.g., participants scored 3.2 out of 5 on average, while non-participants scored 2.8 out of 5 on average).

Two types of impact analysis were conducted:

1. Difference-in-difference (DiD) analysis

2. Intensity of Treatment (IoT) analysis

The DiD analysis compared users and counterfactual both against each other and before and after to assess whether there are statistically significant changes on the three System Questions, and to what extent. The analysis also included individual and time fixed effects, to control for individual variation in responses as well as time-varying factors. The IoT analysis was additional to the DiD analysis, as it assessed whether completing an additional module had an impact on System Question responses. The analysis included the same fixed effects as the DiD analysis. Both analyses were run in R Studio.

As mentioned above, due to the small samples available for this analysis, the results should be interpreted with considerable caution. Lastly, even though we acknowledge that the sample is different in characteristics to the counterfactual sample (and thus not as comparable) the small size prevents us from adding any weights to control for these differences. Any future analysis on this subject should compare samples again and add matching or weighting methods such as propensity score matching (PSM) or inverse probability weighting (IPW) to ensure that impact estimates are robust and accurate.

Educator interviews

Interviews were completed with sixteen educators. Thirteen of these interviews were conducted remotely using MS Teams or telephone. Three were conducted through face-to-face case study visits to schools participating in Cyber Explorers. Data collection started on 6th June and continued throughout July until the end of the school term. Topic guides covered reasons for registering for Cyber Explorers, delivery models, perceived effectiveness of the digital solution, and views on outcomes for educators and learners with a focus on cyber skills and knowledge and awareness of cyber security careers.

Learner focus groups and surveys

It was originally intended to capture learner feedback through school case studies. Three face-to-face case studies were conducted, which involved focus groups with c.20 students at each visit. Many schools struggled to find time to host a focus group with students, due to fieldwork falling towards the end of the summer term. To overcome this barrier, a short online survey was distributed to educators who had provided consent to be contacted about the evaluation. This resulted in online responses from 245 learners. The survey covered which aspects of Cyber Explorers learners found most enjoyable, suggestions for improvement, and future plans relating to computing and cyber security.

Policy interviews

Eight interviews were conducted with relevant policy stakeholders from DCMS and NCSC. These were conducted remotely by telephone or MS Teams and explored how

the programme links to wider policy, how the evaluation can help inform future programmes, and lessons learnt. Interviews were conducted throughout June and July 2022.

Industry and delivery partner interviews

Four interviews were conducted with delivery partners who have been involved in delivering activities and events in pilot areas. Additional face-to-face interviews were completed with seven industry partners who supported a pilot event in one pilot area. Interviews explored differences in how the programme has been delivered across pilot areas, reasons for involvement in the programme, local context, and challenges and enablers to delivery.

Delivery provider interviews

Five remote interviews were conducted with members of the delivery provider team. Interviews explored enablers and barriers to delivery, with a particular focus on lessons learnt relating to the delivery partner model and engagement in pilot areas.

Annex two: Research questions

This annex outlines the research questions identified in the invitation to tender.

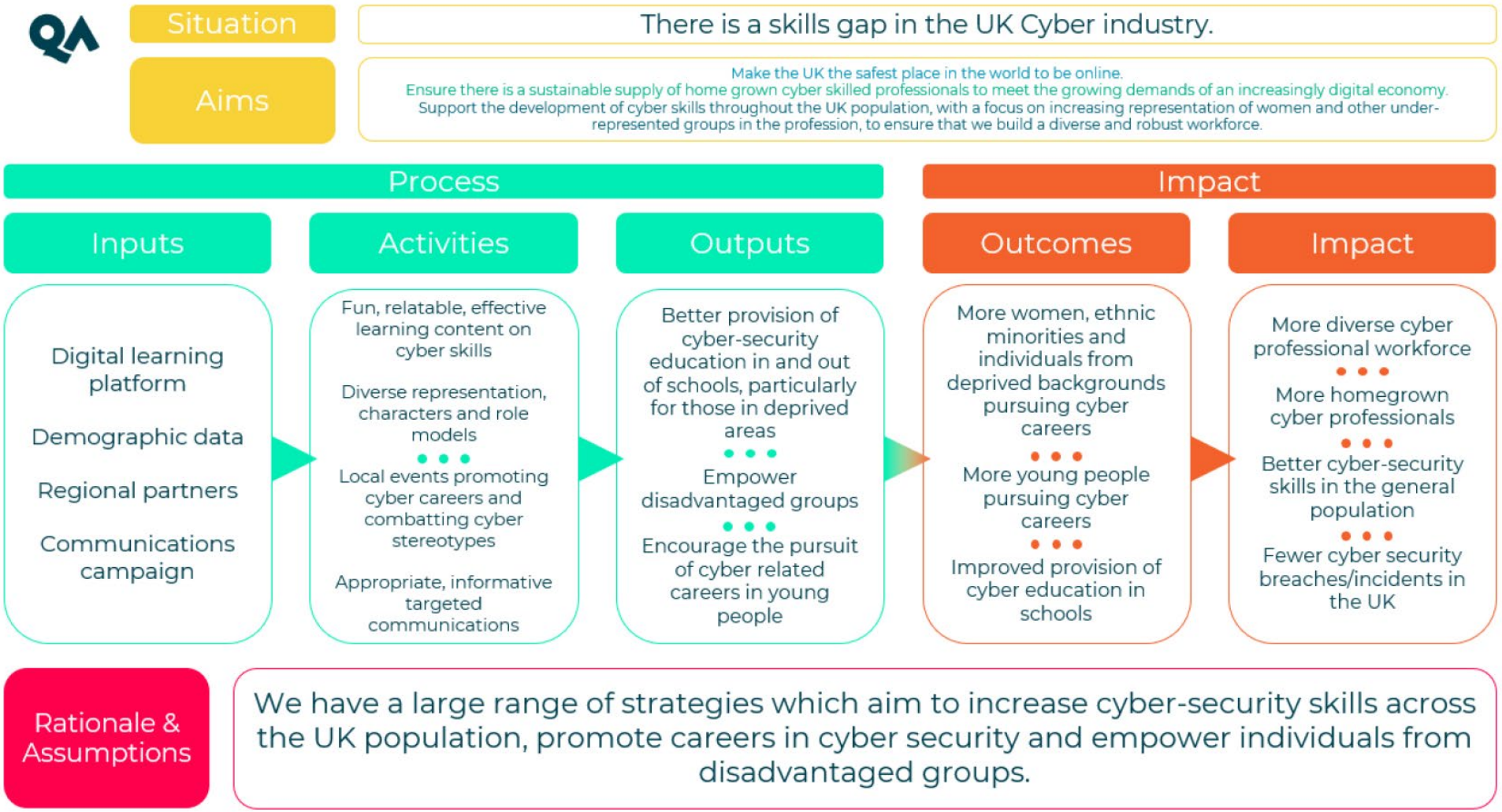
Cyber Skills & Careers Inspiration Programme for Young People		
Type of Question	Area	Question
Process	Programme Delivery	Was the programme delivered as described in the Theory of Change? Were the assumptions laid out in the ToC met?
		How did the rollout of the programme differ across the pilot areas?
		What were the reasons for any differences?
		To what extent has the programme been able to adapt to the varying needs of the pilot areas?
		Have the programme delivery partners met our expectations (goals, KPIs etc)?
		To what extent was the digital platform an effective way of delivering the intervention?
		What were the barriers and enablers to the delivery of the programme and its objectives?
		What has this programme taught us about how similar future initiatives can be improved?
	Diversity	Did the programme achieve its diversity goals and how does it compare to similar programmes and interventions?
		To what extent did the programme penetrate schools of key interest (e.g., State Schools, schools in areas of child deprivation)?

		Was the programme more successful in attracting certain demographics than others and why?
		What worked well in attracting, retaining and engaging different backgrounds and different diversity characteristics?
		What were participants' initial perceptions of cyber careers at the start of the programme and how did these change during participation by different groups?
	Marketing Campaign	What communications channel or mix of channels were most effective in reaching the target audience?
		How much exposure did the target audience have to campaign messages over time (Reach vs Frequency)? Was this enough to drive the desired action?
		What were the key barriers identified along the conversation journey- from awareness to engagement and consideration?
		What motivations and drivers can future campaigns plug into to better engage with the target audience?
		To what extent did the communications campaign impact recruitment and retention of programme participants across the 5 pilot areas?
		What was the impact (if any) of the use on non-financial incentives on participants to encourage engagement?
Impact	Outcomes & Impact	Has the programme inspired participants to take up/consider KS4 computing or computer science?
		To what extent has the programme influenced participants to take up computing or computer science at GCSE level?
		Do pupils and teachers report having greater awareness of digital/cyber careers and pathways towards them?

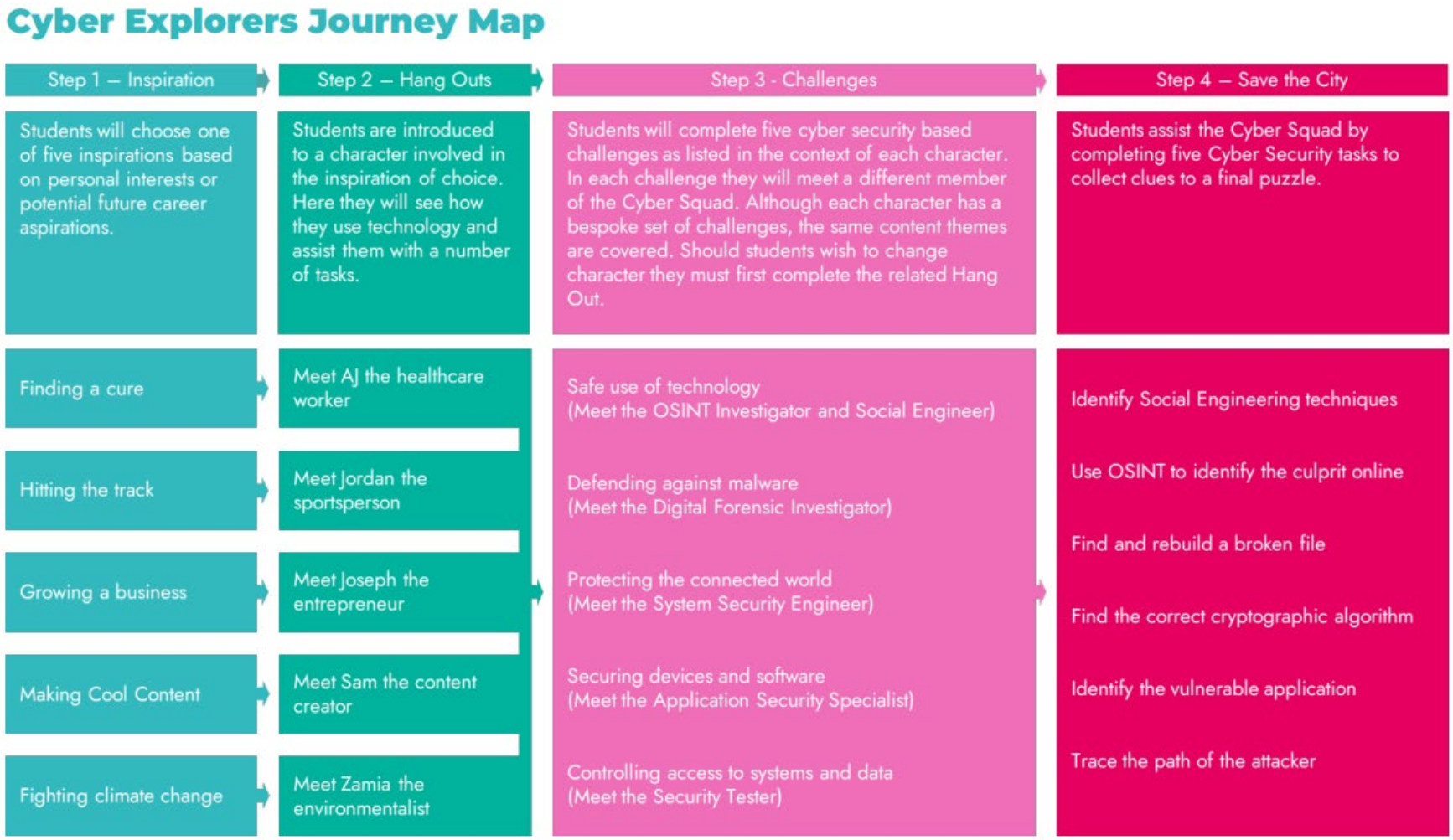
		Do programme participants self-report an improvement in their basic cyber skills?
		What impact has the programme had upon each of its target populations (children, parents, teachers)?
		Did the programme deliver any unintended benefits, or cause any unanticipated adverse consequences?
		To what extent have outcomes differed across the pilot areas, and between pilot and non-pilot areas? What is the strength of evidence about the causes of any differences?
		What was the impact of the five regional pilots?
	Diversity	To what extent has the programme delivered improvements in outcomes for our targeted demographics (girls, ethnic minorities & pupils from low socio-economic backgrounds)?
		Does the programme have greater impact in some demographics than others?
		Is the programme beneficial for diversity?
	Attribution	To what extent can the outcomes delivered be attributed to the programme's interventions?
		What evidence (including secondary data and literature) supports the hypothesis that the initial impacts observed in the intervention (increased intent to do KS4 Computer science, KS4 subject take up) could lead to greater take up and/or consideration of digital and cyber careers at the FE/HE level?
		To what extent do we expect this programme will contribute to a closing of the cyber skills gap over the long term?
	To what extent has the programme delivered value for money?	

Value for Money	To what extent may an increase in resources for communication campaigns deliver improved take up of the programme?
	Which elements of the programme provided the most value?
	What learning could be taken into future programmes to improve returns on investment in the future?

Annex Three: Programme Theory of Change



Annex Four: Cyber Explorers Journey Map



Annex Five: Glossary of terms

Term	Definition
Learner	A young person who has registered and taken part in Cyber Explorers.
Engaged learner	By QA's definition, a learner who has logged in and completed approximately 85% of the Cyber Explorers content (i.e., at least six modules) is defined as 'engaged'. For the purpose of impact analysis, learners are considered to be engaged if they have completed at least one module.
Unengaged learner	A young person who has registered for Cyber Explorers but not completed any content.
Delivery partner	An external partner subcontracted by QA to deliver promotional activities in pilot areas.
Delivery provider	The provider, QA Ltd, contracted by DCMS to deliver the Cyber Explorers programme.
Educator	A member of teaching staff within a school who has registered their student/s for Cyber Explorers. For home schoolers, this would refer to the parent/carer who registered the student for the programme.
Engaged educator	By QA's definition, an educator who has signed up at least 20 students.
Pilot area	Activity was focused on five geographical 'pilot areas' (Bradford, Birmingham, Newry, Newport, and Inverclyde) with a strong emphasis on diversity and inclusion.
Module	As illustrated in the Journey Map (Annex Four), Cyber Explorers content is broken down into eight 'modules': inspirations, hangouts, challenges and 'Save the City'. The term module is used to refer to any individual element of content.
IMD	Indices of multiple deprivation (IMD) are widely used datasets within the UK to classify the relative deprivation of small areas. Multiple components of deprivation are weighted with different strengths and compiled into a single score of deprivation (a score from 1 to 10, with 1 being the most deprived and 10 the least deprived).