



Department for
Digital, Culture,
Media & Sport

Cyber Discovery Evaluation

2021

**Diarmid Campbell-Jack, Helen Bickley,
Johnny Lillis: Ecorys UK**

Contents

List of figures	3
List of tables	3
Executive summary	3
Introduction	6
Policy context	6
Programme development	7
Evaluation overview	11
Aim	11
Methodology	11
Report	13
Outputs: programme participation	14
Student participation	15
Programme	15
Club Leader participation	32
Industry expert participation	35
Student intermediate outcomes	37
Functionality	37
Student outcomes	46
Cyber security	46
Cyber security careers	50
Range of participants	59
Additional Club Leader outcomes	61
Programme impact and the skills gap	63
Perceptions of the skills gap and existing mechanisms	63
Additional mechanisms to close the skills gap	64
Conclusions and recommendations	66
Conclusions	66
Recommendations	67
Appendix One: Theories of Change	71
Appendix Two: Tables and Figures	73

List of figures

Figure 1: Registration by English region for Year Four (per 100,000 13 to 18s)	20
Figure 2: House spent on Cyber Discovery per week (Year Four)	21
Figure 3: Computer Science qualifications (Year Four)	23
Figure 4: Future interest in studying subjects (Year Three)	25
Figure 5: Future interest in careers involving subjects (Year Three)	26
Figure 6: Participation in Cyber Discovery and other programmes (Year Three)	28
Figure 7: Reasons for participation: skills, knowledge, careers (Year Three)	31
Figure 8: Image of Cyber Discovery (Year Four)	40
Figure 9: Perception of cyber security careers (Year Three)	54
Figure 10: Very and fairly interested in career involving each subject (Year Three)	56
Figure 11: Importance of careers information on online platform (Year Three)	59

List of tables

Table 1: Programme participation	16
Table 2: IDACI decile	18
Table 3: Subjects studied or studying (Year Three)	22
Table 4: Club Leader status	33
Table 5: Activities undertaken by Club Leaders	34
Table 6: Knowledge and skills ratings (Year Three)	46
Table 7: Percentage very interested in studying each subject in future (Year Three)	48
Table 8: Knowledge and understanding ratings (Year Three)	52
Table 9: Demographics for participants registered for Assess by year	73
Table 10: Programme awareness and participation	75

Executive summary

Policy context

- The government's National Cyber Security Strategy 2016 set aside £1.9 billion to drive forward the UK cyber security agenda and ensure that the UK is secure and resilient to cyber threats
- Among other initiatives, it recognised the importance of identifying and training young people to enter the cyber security profession and pledged to develop a “self-standing skills strategy that builds on existing work to integrate cyber security into the education system”

Participation

- 23,636 students registered for Cyber Discovery in Year One, growing to 27,903 in Year Two and 35,941 students in Year Three. This dropped slightly to 28,232 in Year Four, perhaps due to the impact of school closures during the COVID-19 pandemic
- The proportion of girls registered for Assess reached a third in Years Three (32%) and Four (33%), compared to a quarter (25%) in Year Two and about a fifth (21%) in Year One. The increase in female participants is largely due to the programme being expanded to 13-year-olds, where a higher rate of female participants was driven by targeted marketing campaigns
- Cyber Discovery engaged a greater proportion of ethnic minority participants than sit computer science school exams
- Participation tended to be highest in the less deprived areas and in the South of England

Engagement

- Those taking part tended to do so as they felt it would be enjoyable and useful. Improving skills was important, with both qualitative and quantitative evidence showing that career consideration was not a major motivating factor
- In the first three years, 590 students took part in the Elite phase and completed SANS professional level 6-day training courses in Years Two and Three. 89 Elite participants achieved GIAC certification in Year Two (93% pass rate) and 124 in Year Three (89% pass rate)
- Participants reported that their experiences of the programme were strengthened by being part of a group, having access to support and guidance, and the extension of the programme during the pandemic. Demands on

students' time, particularly for those sitting exams, were a barrier. During school closures, a minor theme from qualitative research was that access to a suitable computer and internet connection was an additional barrier

- Club Leaders and students found the platform engaging, user-friendly and intuitive. They found the level of challenge appropriate and often welcomed being pushed. A minor theme was that it was sometimes too challenging if students did not have the required soft skills and interest in cyber security

Cyber careers

- Students generally had a very positive view of cyber careers, with most agreeing that they were important for society (94%), suitable for someone like them (80%), and open to anyone regardless of background (66%)
- Students were more likely to get information on cyber security careers from Cyber Discovery than from other sources, and after taking part most felt they understood the requirements for pursuing a cyber career
- Survey data suggested that the programme increased skills in computer science and cyber security. There was no evidence that it increased interest in cyber security as a study subject or as a career – this may be due to study methodology or increased knowledge leading some participants to realise that they did not wish to pursue cyber further. Equally, it may reflect the initial objective of the programme which was to engage an elite cohort of most talented young people, rather than appeal to a wider audience

Additional outcomes

- For industry experts, outcomes centred around the potential for recruitment, including the opportunity to meet talented students and raise awareness of cyber security roles
- Club Leaders and industry experts generally felt it was possible that the programme could contribute towards longer-term impact and closing the cyber security skills gap
- Club Leaders were split as to whether Cyber Discovery needed to be linked to the curriculum. A common theme was that content enhanced the curriculum and met the needs of students seeking to broaden their knowledge and skills

Introduction

In January 2018, Ecorys (together with partners at the University of Kent) were commissioned by SANS Institute (the Cyber Discovery “delivery partner”) to evaluate the Cyber Discovery programme (the “programme”) that was launched in November 2017. This report covers all four years of the evaluation. It incorporates results from several strands of data collection, most notably feedback from young people participating in the programme, Club Leaders, school staff and industry experts. Management Information (MI) was provided by the delivery partner.

Policy context

The government’s “National Security Strategy and Strategic Defence and Security Review 2015”¹ set aside £1.9 billion to drive forward the UK cyber security agenda. Shortly afterwards, the government published the National Cyber Security Strategy, stating that the UK required a “self-standing skills strategy that builds on existing work to integrate cyber security into the education system”. Among other initiatives, this outlined the need for a schools programme to create specialist cyber security education/training for talented young people aged 14 to 18, support the accreditation of teachers’ professional development in cyber security, and embed cyber security as an integral part of relevant courses throughout education by 2021.

Analysis of the UK skills gap² shows that approximately 680,000 businesses (50%) have a basic technical skills gap (48% in 2020 and 54% in 2019) and 449,000 (33%) have a more advanced skills gap, most commonly in areas such as penetration testing, forensic analysis and security architecture. The size and nature of any future skills gap in the UK may well be impacted not only by the growing importance of digital literacy and the understanding of cyber security for the workforce,³ but also by the increasing legal obligations on operators in some sectors to improve cyber security standards and by the potential impact of the UK leaving the EU on the ability to access specialist skills from the EU and beyond.⁴

¹ [National Security Strategy and Strategic Defence and Security Review 2015](#)

² [Cyber Security Skills in the UK Labour Market, 2021](#)

³ [Initial National Cyber Security Skills Strategy](#)

⁴ [Joint Committee on the National Security Strategy](#)

Programme development

The programme has run for four years: Year One (2017/18), Year Two (2018/19), Year Three (2019/20) and Year Four (2020/21), with this section of the report outlining how the programme has developed over this period.

Year One development

In February 2017, the Department for Culture, Media and Sport (DCMS) announced plans to invest £20 million in an “ambitious Cyber Schools Programme” as part of the Government’s CyberFirst⁵ initiative. The programme was to meet the “critical need to increase the availability of cyber security skills”,⁶ recruiting 14 to 18 year-olds with the motivation and aptitude for a programme that was “expected to mix classroom and online teaching with real-world challenges and hands-on work experience”.⁷ The programme “aims to capture the imagination of young people and inspire them to consider a career in cyber security, while identifying and nurturing promising talent from a young age”.⁸ The initial objective was to ensure a minimum of 600 people completing a year’s equivalent [of] for all aspects of ‘blended learning’ content in the pilot phase (Year One), scaling up each year to reach the total target of 5,700 programme participants by 2021.

The initial programme consisted of four stages:

- **Assess:** An introductory set of 14 problem-solving challenges, designed to assess existing cyber security knowledge and skills. This phase was a programme delivery requirement, included to ensure only those with latent or existing skills could qualify for the learning phases of the programme
- **Game:** Hundreds of hours of gamified challenges across several content-specific ‘bases’, providing realistic examples of tests and threats faced by cyber security practitioners in the field
- **Essentials:** A set of interactive lab exercises, videos, exams and quizzes aiming to provide the theoretical knowledge behind advanced cyber security topics
- **Elite Camp:** A set of regional face-to-face residential camps for ‘elite’ students (the highest achieving performers through previous stages⁹). Camps provided further

⁵ CyberFirst is delivered by NCSC and aims to develop “the UK’s next generation of cyber professionals through our student bursaries, courses for 11-17 year-olds and competitions”. This includes Cyber Discovery, Cyber First Girls Challenge and the Cyber Schools Hub. Further details can be found at the [CyberFirst Girls Competition webpage](#).

⁶ [Cyber Schools Programme Guidance](#)

⁷ [Search to find Cyber Security experts of the future, press release](#)

⁸ [Initial National Cyber Security Skills Strategy: increasing the UK’s cyber security capability - a call for views, Executive Summary](#)

⁹ In Year One, ‘elite students’ were defined as students scoring 13 or 14 on CyberStart Assess (out of a maximum possible score of 14), having broken into HQ level 10 and 11 (completing at least one challenge

cyber security training, inspirational talks, careers advice and hands-on activities provided by the delivery partner with the support and involvement of industry experts

The primary programme objective was to identify highly talented young people and to further develop their skills, helping fast-track them into relevant roles. A secondary aim was to engage a broader base of participants, to engage those with general skills and understand how they can be engaged and progress through the programme. In addition, the programme aimed to encourage participants to consider cyber security as a career through embedding relevant information throughout the platform, industry participation at the Elite Camp, and school visits and events.

In Year One, the programme was only offered in England. Students could either take part as individual members in their own time, or they could join as part of a Cyber Discovery club. Clubs required a Club Leader (often a teacher), who would generally run the club as an extra-curricular activity. Club members could also work on challenges in their own time. Where this report refers to individual and club members, it indicates the two different paths for registering for the programme.

Year Two development

Changes made for Year Two included the roll-out of the programme across the whole of the UK, bringing programme dates forward to avoid/reduce overlap with exam periods; increasing the qualifying score required to move to Game (from six to eight at Assess phase); including fourteen new challenges for the Assess phase and a new online module within Game covering Digital Forensics; a focus on “driving more female interest and participation in a bid to challenge the industry’s gender gap”¹⁰; and the introduction of a series of 6-day residential camps as the Elite phase. SANS training was delivered for the first time, leading to GIAC certification attempts, plus a series of industry sessions, soft skills workshops and networking opportunities, hosted at university campuses across the country.

Year Three development

As the original target KPI of achieving 5,700 participants was met in Year One alone (registrations for Assess at 21,834 in Year One, 25,904 in Year Two), it was hoped the programme would reach 30,000 participants in Year Three, with a similar increase from 160 to 240 in Elite Camp participants.

in both) and having “demonstrated keen interest in the cyber security industry” (*Cyber Discovery Year 2 Close Of CyberStart Assess Report*).

¹⁰ SANS management information; “Cyber Discovery Year Two: Close of Game and Essentials Report”, p12

Cyber Discovery's entrance criteria were amended to allow young people aged 13 to take part. Content was updated, with key changes being:

- Assess: new challenges developed and implemented
- Game: new content module added (Volcano base), with this being the most technically advanced content in the phase to date
- Essentials: content updated to make more user-friendly, primarily replacing audio with video and updating the visuals in the final quiz
- Elite: moved from face-to-face to entirely online delivery due to COVID-19. The content was kept similar to Year Two. The move to online delivery required logistical changes, mainly relating to safeguarding and supporting participants. An additional GIAC exam was also introduced in Year Three, covering Intrusion Detection (SEC503)

A Talent Development Programme (TDP) was introduced during Year Three. The Programme aimed to give the very top Elite phase performers access to additional SANS courses to develop their skills to a professional level. TDP participants were also supported by mentors from the cyber security industry, including SANS.

Year Four development

A Virtual Cyber School was introduced in May 2020 to provide ongoing activity during the COVID-19 period from May to August 2020. Participants could test their interest in cyber security through the School and then access the Year Four Assess phase when this opened in June 2020.

Assess opened in Year Four earlier than in previous years (June 2020) to provide continued learning during the pandemic. Online workshops were introduced to supplement school visits. These took place in the first eight weeks of the 2020/21 school year and reached approximately 3,700 students.

In Year Four Elite Camps were replaced with a final event, consisting of industry panel discussion, careers advice, and a Capture The Flag (CTF) challenge. The event was hosted online, with 500 students invited to attend.

Theory of Change

A Theory of Change was developed with key stakeholders (SANS and DCMS) at the outset of the evaluation in 2018. This was subsequently revised in Summer 2020 with particular focus on identifying programme assumptions. Both versions are included in Appendix One.

Inputs

There were no significant changes in Cyber Discovery systems or staffing. Changes to overall delivery and timings are covered in the 'Programme Development' chapter above.

Activities

Promotional activity was refined in Years Two, Three, and Four based on the learning outcomes of previous campaigns. Direct mailings into schools were not possible in the run up to Year Four, due to closures as a result of COVID-19, so promotion was focused on social media and other online media. There was a continued focus on driving gender diversity throughout the programme, as well as specific geo-targeted campaigns to encourage uptake in economically disadvantaged areas.

Evaluation overview

Aim

Ecorys were commissioned in January 2019 to deliver the evaluation in partnership with the University of Kent. The final aims of the evaluation were to:

- Assess the impact on participating students and Club Leaders, and whether it has been successful in raising awareness, interest, and engagement in cyber security careers
- Identify what worked well and less well with the programme and if it has achieved and is on track to achieve its aims and objectives, including success factors
- Assess the impact on the cyber security industry
- Develop and conduct an economic analysis to demonstrate value for money

Methodology

A mixed methods approach was adopted, involving both quantitative and qualitative data collection. Data collection included the following:

	Data collection
Year One	<ul style="list-style-type: none">● Management information
Year Two	<ul style="list-style-type: none">● Management information● Club Leader “call for evidence”: short online survey focussing on gender diversity (n=106)● Case studies to school-base clubs (n=4): interviews with Club Leaders, students, management and career staff● Telephone interviews with Club Leaders (n=12)● Telephone interviews with industry experts: experts who had engaged with Cyber Discovery (n=6) and other experts from outside the Programme (n=10)● Case study visits to Elite Camps (n=3): interviews/focus groups with participants, observation of Elite Camp sessions, interviews with Club Leaders and industry experts, follow-up telephone interviews with parents of Elite Camp attendees
Year Three	<ul style="list-style-type: none">● Management information

	Data collection
	<ul style="list-style-type: none"> ● Pre and post-surveys: pre sent to all Assess participants shortly after the beginning of Year Three (Oct-Nov 2019, n=595). Post sent to all pre-survey respondents who had agreed to be recontacted with post-survey (Sept-Oct 2020, n=115) ● Club Leader mini survey: short online survey focusing on cyber security careers (n=69) ● School case study visits (n=4): interviews/focus groups with students (n=18), Club Leaders (n=4), and other school staff (n=3) ● Telephone interviews with non-club participants (n=4) ● Telephone interviews with Elite Camp students who sat GIAC exams (n=4) ● Telephone interviews with industry stakeholders (n=4)
Year Four	<ul style="list-style-type: none"> ● Management information ● Single point in time survey: sent to all current Game participants and all participants who had previously taken part in Year Four Game (n=196) ● Long-term follow-up survey: small-scale survey focusing on open text qualitative data sent to all Year Three post-survey respondents who had agreed to be recontacted for future research (n=33) ● Previous participant online focus groups (n=2) ● Current participant online focus groups (n=6) ● Telephone interviews with Club Leaders (n=8) ● Telephone interviews with curriculum experts (n=8)

The Year Four single point in time survey repeated some questions asked at the Year Three pre-survey, but throughout the report we focus on Year Three responses. This is because the Year Three pre-survey had a larger base size and was distributed at the Assess stage, so is likely more representative of the overall participant population. Results were broadly similar across the two surveys, but where there are notable differences we have reported both years. Due to issues of timing, it was not possible to conduct a pre and post-survey in Year Four, so a single point in time survey and long-term follow-up survey were designed to support Year Three findings.

Report

This report provides feedback from stakeholders across the overall Theory of Change (see Appendix One) and covers outputs, student intermediate outcomes, student and Club Leader outcomes, student impact and a final section outlining conclusions and recommendations.

Data limitations

- Some of those taking part in data collection activities (particularly Club Leaders) were not always able to distinguish clearly between programme years
- The absence of a counterfactual (data showing what would have happened for a similar group who had not taken part in Cyber Discovery) means we cannot prove whether any positive or negative changes identified in the evaluation would have happened anyway without the programme. The feasibility of a counterfactual was examined in the early stages of the evaluation but was not possible due to budget and the limits to data collection at the registration stage
- Results from the Year Three pre and post-survey and the Year Four single point in time survey are not directly comparable. The Year Three pre-survey took place before the Game stage, while the Year Four survey took place when the Game stage had started.¹¹ Data suggests that respondents to the Year Four survey were more engaged, as may have been expected if the survey timing meant those who had not reached Game were less likely to respond

¹¹ This is supported by analysis of self-reported interest in cyber security on a scale of one to ten: the mean for Year Three pre-survey was 7.8, compared to 9.4 for Year Four single point survey.

Outputs: programme participation

Summary

Management Information participation levels

- Cyber Discovery exceeded its target of engaging 5,700 people across all four years in Year One alone
- Assess registrations increased across the first three years, from 21,834 in Year One to 25,904 in Year Two and 33,427 in Year Three
- Assess registrations were lower in Year Four (28,232). This decrease was largely explained by a reduction in club members, likely due to fewer teachers running clubs in the context of COVID-19 disruptions to schools
- In the first three years, slightly over half of participants were club members, decreasing to 41% in Year Four
- The programme achieved its soft target of 30% female participants in Years Three (32%) and Four (33%). This was partly due to changes in admissions policies and promotion at Year Three: the programme was expanded to accept 13-year-olds, and promotional activity focused on 13-year-old girls in particular
- MI shows a geographical pattern of higher levels of registration towards the South of England than in the North. Evidence suggests participation is higher among students in less deprived areas than those that are more deprived

Evaluation data on student profiles

- Pre-survey data showed most students (81%) had or were studying computer science, with high proportions being very (43%) or fairly (44%) interested in studying cyber security in the future
- Interest in studying or having a future career in cyber security tended to be higher among males than females and among those at state school rather than private or other schools
- Those taking part tended to do so as they felt it would be enjoyable and useful. Improving skills was important for participants, with careers related reasons being less so

Student participation

The initial stages of the programme involve engaging potential young people and Club Leaders. The programme aimed to work with a demographically diverse group of participants, and provide them with content that they could not get elsewhere, thereby attracting talented and interested students.

Promotional approaches taken

Recruitment for Cyber Discovery involved both broad-based and targeted approaches to schools (see “Activities” section), with non-school staff also able to find information online and register to become a Club Leader.

For Club Leaders, distribution of print material in schools was the largest driver of teacher sign ups, followed by direct e-mails to teachers using purchased teacher lists. Evaluation data also showed that Club Leaders commonly heard about Cyber Discovery through social media, in particular Twitter, or from students who heard about the programme and wanted their school to participate. Some Club Leaders had previous involvement in the CyberFirst Girls Competition or worked in CyberFirst accredited schools and were made aware through e-mails from CyberFirst.

Throughout the evaluation, Club Leader feedback suggested that the marketing pack was appreciated, primarily as it made it easy for staff to advertise the programme to students.

“Ready-made flyers and posters save teachers’ time and make things a lot easier for them to promote the programme.” Club Leader

In Year Four there was more reliance on digital materials, such as e-mails and e-flyers which could be uploaded onto school intranets, due to school closures in response to the COVID-19 pandemic.

Programme

MI data was collected for all participants in each year on key demographic information including age, gender, ethnicity, and region. This section presents total participation numbers across the programme duration and also examines diversity across different demographic characteristics.

Total participation

The programme aimed to have at least 5,700 people complete or engaged by the end of 2021. As shown by Table 1, Cyber Discovery exceeded this participation target in Year

One alone, and achieved over 100,000 registrations across the four years.¹² Assess registrations increased from 21,834 in Year One to 25,904 in Year Two and 33,427 in Year Three.

The consistent increase in registrations over the first three years suggests that Cyber Discover was effective at growing its participant base before the COVID-19 period. In Year Four registrations decreased to 28,323 from 35,941 in the previous year. While the number of individual participants decreased only slightly from 16,657 in Year Three to 15,711 in Year Four, club members showed a larger reduction from 17,716 to 11,575. The drop in club members is most likely due to school closures resulting from the COVID-19 pandemic, which reduced opportunities for teachers to run face-to-face clubs and meant students were less able to access extra-curricular activities.

Table 1: Programme participation

	Year One	Year Two	Year Three	Year Four
Registered Cyber Discovery	23,636	27,903	35,941	NA ¹³
Registered Assess	21,834	25,904	33,427	28,232
Registered Game ¹⁴	7,146	5,320	10,564	7,471
Registered Essentials	3,759	3,851	3,497	3,250
Identified as 'Elite' ¹⁵	287	487	624	778
Attended Elite Camp	170	180	240	NA ¹⁶

Source: Management Information.

Sub-group participation

Understanding the extent that different types of people take part in Cyber Discovery is important given the outcome in the Theory of Change to engage a suitably diverse range of participants. This section uses MI data to analyse the profiles of Cyber Discovery

¹² This includes some participants registering in multiple years.

¹³ Unlike in previous years, there was no pre-registration campaign in Year Four due to it opening earlier in the year. As a result, everyone who registered in Year Four gained instant access to Assess.

¹⁴ Game registrations as a percentage of all registrations dropped between Year One and Year Two as the qualification bar was raised.

¹⁵ In Year One, 'elite students' were defined as students scoring 13 or 14 on CyberStart Assess (out of a maximum possible score of 14), having broken into HQ level 10 and 11 (completing at least one challenge in both) and having "demonstrated keen interest in the cyber security industry" (*Cyber Discovery Year 2 Close Of CyberStart Assess Report*).

¹⁶ There was no Elite Camp in Year Four.

participants, including any changes across the four years. Full MI data on participation is presented in Table 9 of Appendix Two.

Encouraging diverse engagement

Gender

From Year Three onwards, a soft target was set to have females make up 30% of all participants. In Year One roughly one fifth (21%) of those registering for Assess were female, rising to a quarter (25%) in Year Two and a third in Years Three and Four (32%, 33%). The target was surpassed in Year Three and Four due to the programme in these years being expanded to those aged 13: in both years, 42% of 13-year-olds registering were female. For participants aged 14 to 18, the percentage who were female was 28% in both years. Therefore, while there was a slight increase in the percentage of female participants across all ages at Years Three and Four, it was mostly driven by higher proportions of 13-year-old female participants.

The Year Two Club Leaders survey asked all leaders their satisfaction with how Cyber Discovery engaged each gender. Leaders were equally satisfied with how the programme engaged females (30% very satisfied) and males (44%), with there not being any statistically significant difference in endorsement. Most of the remaining leaders were quite satisfied with how the programme engaged females (37%) and males (35%), with relatively few being unsatisfied (9% for females and 2% for males).

Club Leaders were generally positive in interviews about the ways that Cyber Discovery engaged females. One felt that it was challenging to get girls to take part in computing, but that the programme had been very successful as it took an open approach and started at a relatively basic level. They noted that unlike more technical elements of computing (such as Raspberry Pi), those taking part did not have to quickly get up to speed with technical demands. Similarly, one Club Leader felt that without the programme *"there's no way we'd have the number of girls interested in this area that we do. It's made a big impact."* A major theme was Club Leaders feeling that the programme was *"fairly neutral"* and *"not really appealing more to one gender or another"*.

Ethnicity

MI data show that Cyber Discovery has a higher proportion of ethnic minority participants than those taking part in Computer Science at school. In total, 29% of Cyber Discovery participants were ethnic minority students which is higher than the percentage of 2017 ethnic minority students GCSE (22%) and A-level (25%) participants.¹⁷ In total for both Years Three and Four, two-thirds (67%) of participants defined themselves as white, one-

¹⁷ [The Roehampton Annual Computing Education Report: Data from 2017](#)

fifth (19%) as Asian, 5% as Black, 4% as Mixed and 2% as Other. A further 5% of participants did not provide information on their ethnicity.

Deprivation

Postcode data from schools was linked to the Income Deprivation Affecting Children Index (IDACI). IDACI measures the proportion of children aged 0 to 15 living in income deprived families^{18,19}. This is used to categorise schools into IDACI deciles, with those in decile 1 being the most deprived 10% of English neighbourhoods and those in decile 10 the least deprived.²⁰ Schools postcode data was only available for Years Three and Four, and is presented in the following table.

Table 2: IDACI decile

	Year Three	Year Four
1 – most deprived	7%	7%
2	8%	8%
3	9%	9%
4	10%	9%
5	10%	9%
6	11%	10%
7	10%	10%
8	11%	11%
9	11%	12%
10 – least deprived	14%	14%
<i>Base: Total sample</i>	(2,878)	(2,615)

Source: Management Information.

¹⁸ [LG Inform, IMD IDACI score England](#)

¹⁹ This is used as a proxy measure due to the different age groups: Cyber Discovery being open to young people from 13-18, while IDACI provides data for those aged 0-15.

²⁰ For Year Three, details were provided for 3,393 schools, of which 2,891 were in England and 2,878 were successfully matched to IDACI deciles. For Year Four, details were provided for 3,011 schools, of which 2,621 were in England and 2,615 were successfully matched.

Analysis of school postcodes shows that in terms of levels of deprivation, Cyber Discovery engaged similar schools in Years Three and Four. In both years, schools were more likely to be located in less deprived areas: two thirds of schools (66%) taking part in Cyber Discovery were situated in the top five least deprived deciles. Further analysis showed that 74% of schools were state schools and 12% were independent, with no information on school type available for the remaining 14%.

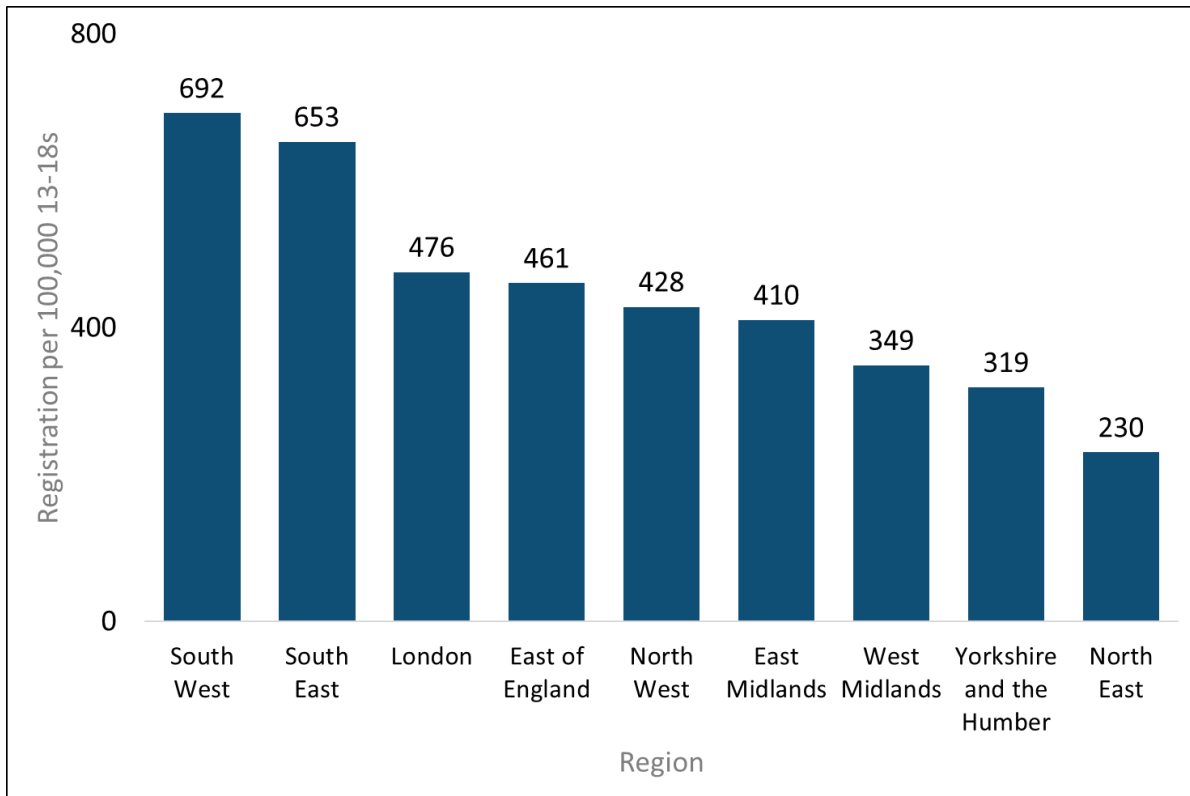
Geographical spread

In Year One the programme was only available to participants in England, but in Year Two it could be accessed in the devolved nations. In Year Two, 93% of participants were from England which decreased to 88% in both Year Three and Year Four. Outside of England, participants were most likely to take part from Scotland (7% Y3, 8% Y4), followed by Wales (3% Y3, 3% Y4) and Northern Ireland (2% Y3, 1% Y4). These results were broadly in line with population distribution across the four nations.²¹

Data on registration by English region for Years Three and Four, showed a similar pattern of uneven engagement across different English regions. To ensure comparability, figures were calculated to show the number of Cyber Discovery participants out of each 100,000 13 to 18 year-olds in each region, with Figure 1 showing data for Year Four.

²¹ [Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2019](#)

Figure 1: Registration by English region for Year Four (per 100,000 13 to 18s)



Source: Management information. Base: 28,232.

The regional figures show higher levels of registration in the South of England, particularly in the South West (692 participants per 100,000 13 to 18 year-olds) and South East (653). Rates were particularly low for the North East (230) and Yorkshire and the Humber (319), with Cyber Discovery generally engaging lower proportions of participants in the North of England.

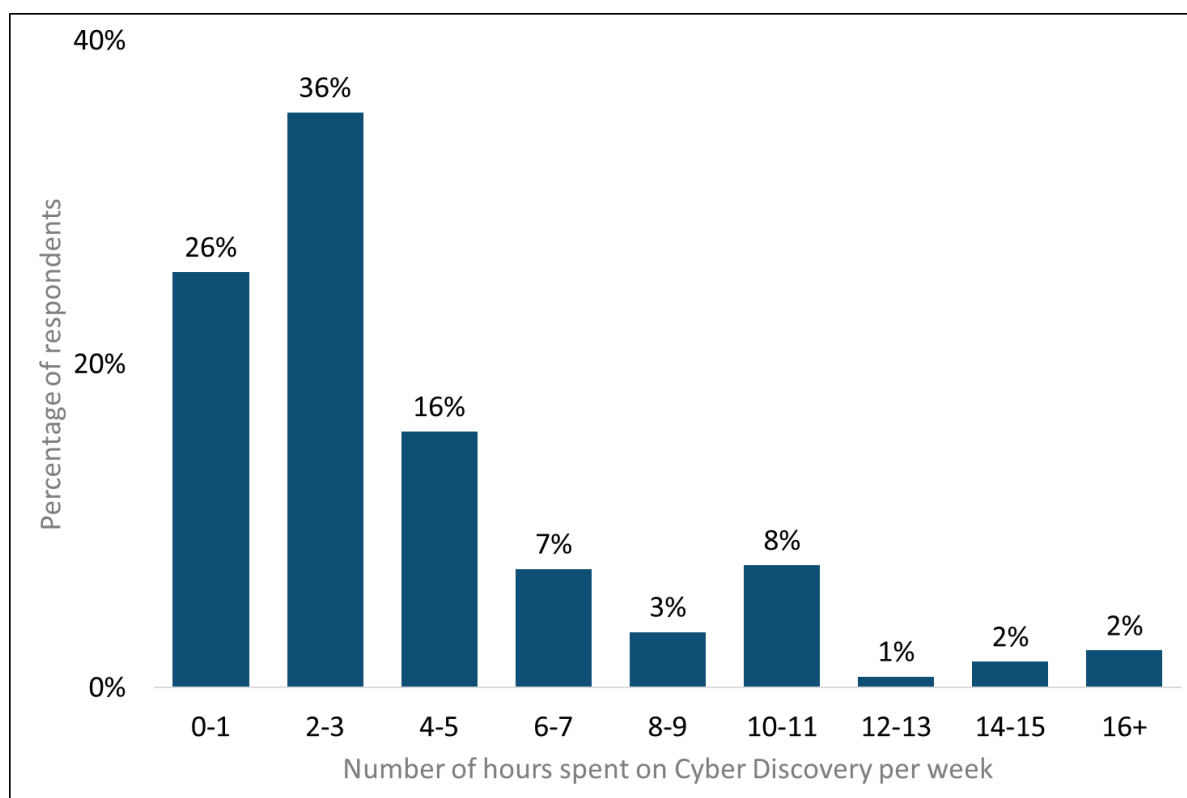
Elite Camp and GIAC exams

Most students who sat the GIAC exams passed, with pass rates of 93% in Year Two and 89% in Year Three. The mean score achieved was 85% in both years, with 28% and 53% achieving a score of at least 90. The exams are aimed at adults, with anyone scoring over 90% in any course being invited onto the GIAC advisory board, and a score of over 95% placing one in roughly the top 5% of those sitting the exam.

Time spent on Cyber Discovery

At the Year Four single point survey, respondents were asked to estimate how many hours they spent on Cyber Discovery since the start of Game, both in their own time as individual participants and as part of a club. The following figure shows the total time that each respondent spent per week on Cyber Discovery.

Figure 2: Hours spent on Cyber Discovery per week (Year Four)



Source: Year Four single point survey. Base: 196.

On average, respondents spent 4 hours a week on Cyber Discovery, although there was considerable variation. Over half of respondents (62%) spent three hours or less a week on Cyber Discovery, with a quarter (26%) spending up to one hour a week and a third (36%) spending two to three hours a week. There were a small proportion of respondents (15%) who spent at least eight hours a week on the Programme.

Impact of COVID-19 pandemic on time spent on programme

Respondents generally felt that the COVID-19 pandemic meant they spent more time on Cyber Discovery than would have happened otherwise. Nearly half of respondents (45%) said they would have spent less time on the programme if the COVID-19 pandemic had not occurred, while a quarter (25%) said they would have spent more time. The remaining third (30%) judged that the amount of time they spent on the programme would not have changed. Only a very small proportion (6%) felt that they would not have taken part in the programme at all, if it were not for the pandemic. Most people (93%) felt that COVID-19 had not impacted the amount of time they spent on Cyber Discovery as part of a club, with only 6% saying they would have spent more time on clubs if it weren't for the pandemic.

Subject choice

The Theory of Change notes the importance of both identifying the most talented and engaging people who are less likely to be “usual” suspects, for example those who do not have STEM backgrounds. While ability and talent are not assessed as part of existing programme Management Information, survey data on subjects people have studied or are considering studying contributes to understanding the type of participants who engage in the programme. Most participants (81%) had studied Computer Science at some level, indicating the participants generally had some base knowledge and interest in computing.

Subjects studied

The following table shows the percentage of Year Three pre-survey respondents who had studied each subject at different qualification levels. Patterns were broadly similar for Year Four respondents, although they were slightly more likely to have studied Science, Maths, and Computer Science at all levels, which may be due to the higher proportion of older students in the Year Four sample compared to the Year Three pre sample.

Table 3: Subjects studied or studying (Year Three)

	Science	Maths	Computer Science	Design and Technology	ICT
GCSE, NVQ or equivalent	76%	75%	71%	30%	20%
AS, A Level or equivalent	17%	24%	20%	2%	3%
Above AS or A Level or equivalent	2%	3%	3%	1%	1%
Not studied	15%	14%	19%	64%	72%
<i>Base: Total sample</i>	<i>(595)</i>	<i>(595)</i>	<i>(595)</i>	<i>(595)</i>	<i>(595)</i>

Source: Year Three pre-survey.

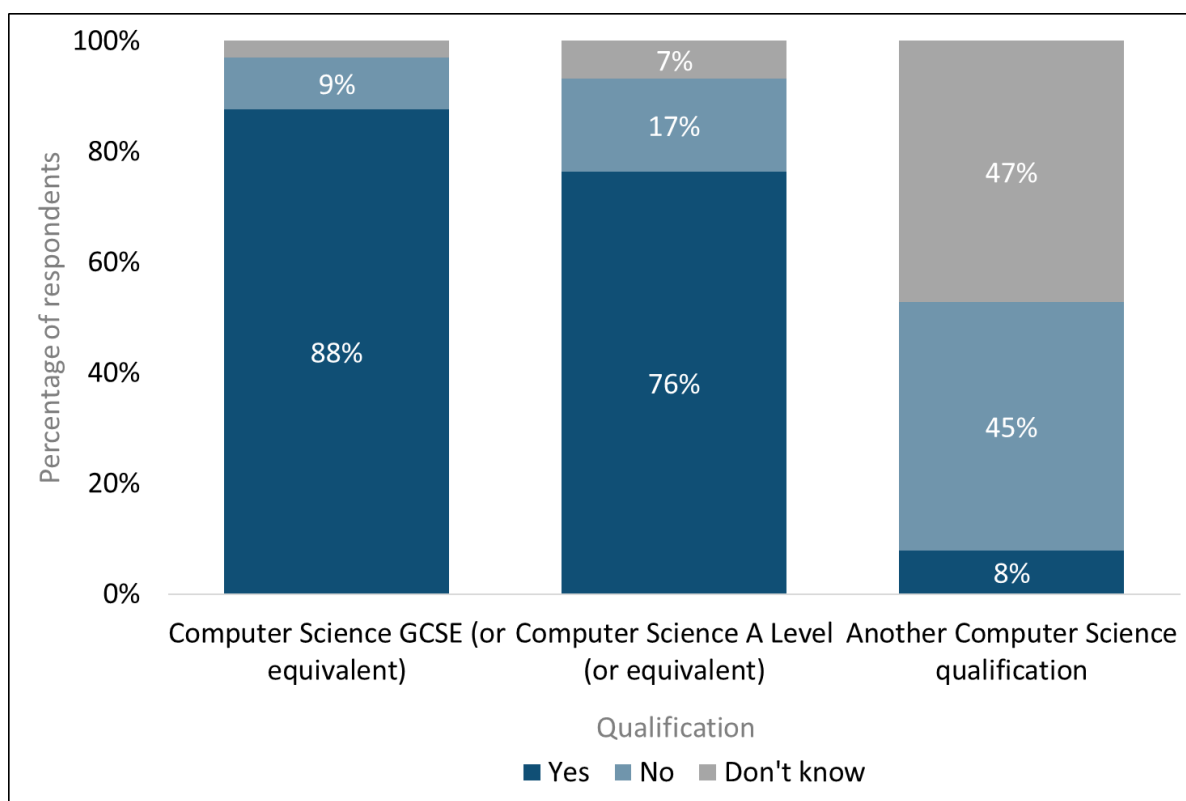
Over two-thirds of respondents had at least some prior experience of computer science in general, with 71% having studied towards a Computer Science GCSE or equivalent and 20% having studied towards an A Level or equivalent. This shows that most Cyber Discovery participants had an interest and understanding in Computer Science. Club Leaders said in interviews that they often deliberately targeted these classes when looking for Cyber Discovery participants, and that they saw the programme as well suited to students with strong logical reasoning, particularly Maths students. Individual

participants were on average older than club participants and therefore more likely to have studied towards computer science qualifications, but after controlling for age there was no difference in the proportion of individual and club participants who had studied computer science at any qualification level.

School Computer Science provision

Those taking part in the Year Four single point survey were asked what Computer Science qualifications were offered to respondents by their school, as outlined in Figure 3.

Figure 3: Computer Science qualifications (Year Four)



Source: Year Four Single Point survey. Base: 196 (GCSE, A-level); 182 (Another qualification). Data label not shown for Computer Science GCSE, Don't know (3%).

Nearly nine out of ten respondents (88%) reported that their school offered Computer Science GCSE (or Scottish equivalent), and three-quarters (76%) said that their school offered it at A Level (or Scottish equivalent). By comparison, research from 2018 showed that 79% of Year 11 students were in schools which offered Computer Science GCSE.²² This shows that those taking part in Cyber Discovery are more likely to come from schools which offer Computer Science.

²² [The Roehampton Annual Computing Education Report: Pre-release snapshot from 2018](#)

Interviews suggested that some students took part in Cyber Discovery who were not studying Computer Science, although their school offered the qualification. Reasons for this included dissatisfaction with the curriculum content or teaching styles. Some noted that Computer Science qualifications contained minimal content relating to cyber security, so the opportunity to enhance their skills was a significant reason for taking part in Cyber Discovery.

A small proportion of respondents (8%) indicated that their school offered another Computer Science qualification, and were prompted to provide more information on the qualification. Several schools offered BTECs, with other qualifications mentioned including Oxford Cambridge and RSA (OCR) Technical Level 3 Information Technology and OCR Entry Level Computer Science.

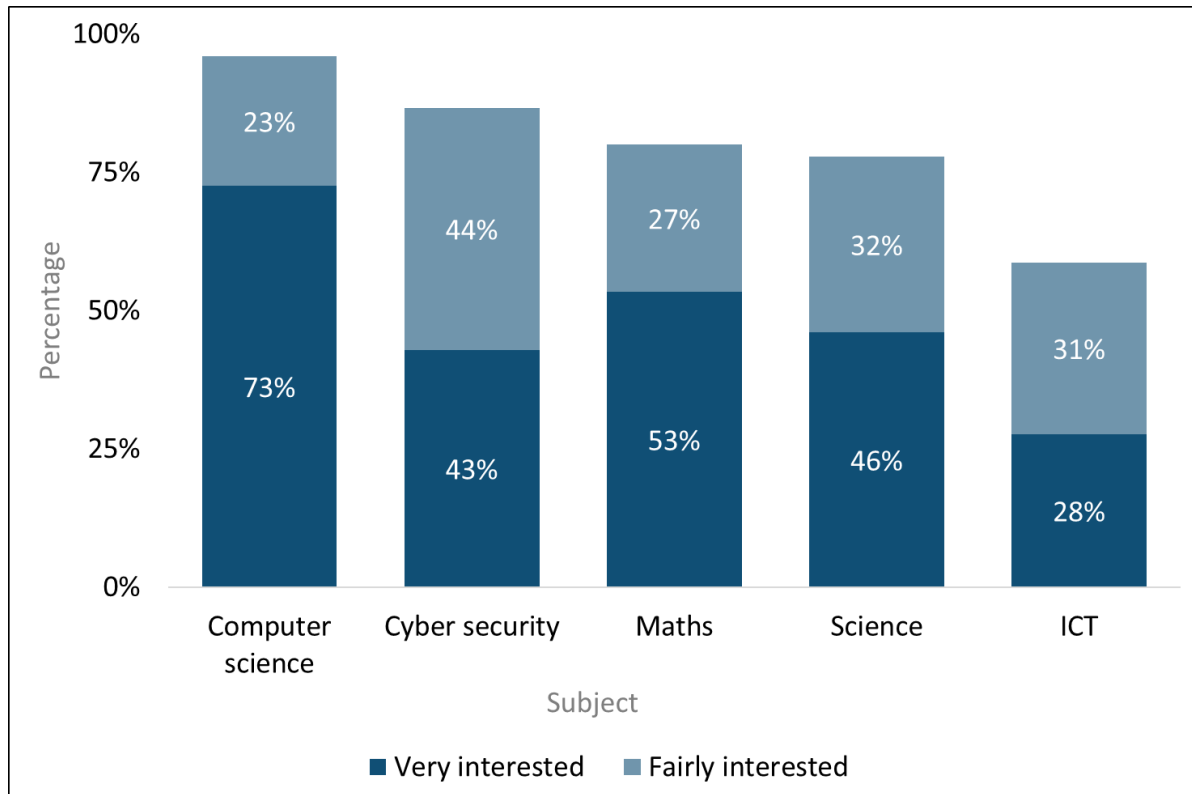
Interest in STEM and non-STEM subjects

Respondents taking part in the Year Three survey were asked their interest in STEM subjects, humanities, and creative subjects. Respondents were very interested in STEM subjects, giving this an average score of 9.8 on a scale of one to ten where one was not at all interested and ten was very interested. This compared to a mean score of 5.1 for humanities and 5.5 for creative subjects.

Interest in studying subjects in future

At the Year Three pre-survey, respondents were asked how interested they were in studying certain subjects in the future, with results shown in the following figure.

Figure 4: Future interest in studying subjects (Year Three)



Source: Year Three pre-survey. Base: 595.

Almost all Cyber Discovery participants were interested in studying computer science, but they were also interested in a range of other subjects. Just under half (43%) of respondents said that at the start of the academic year they were very interested in studying cyber security in the future, with a similar proportion (44%) being fairly interested. Most of the remainder were not very interested (12%) rather than not at all interested (2%).

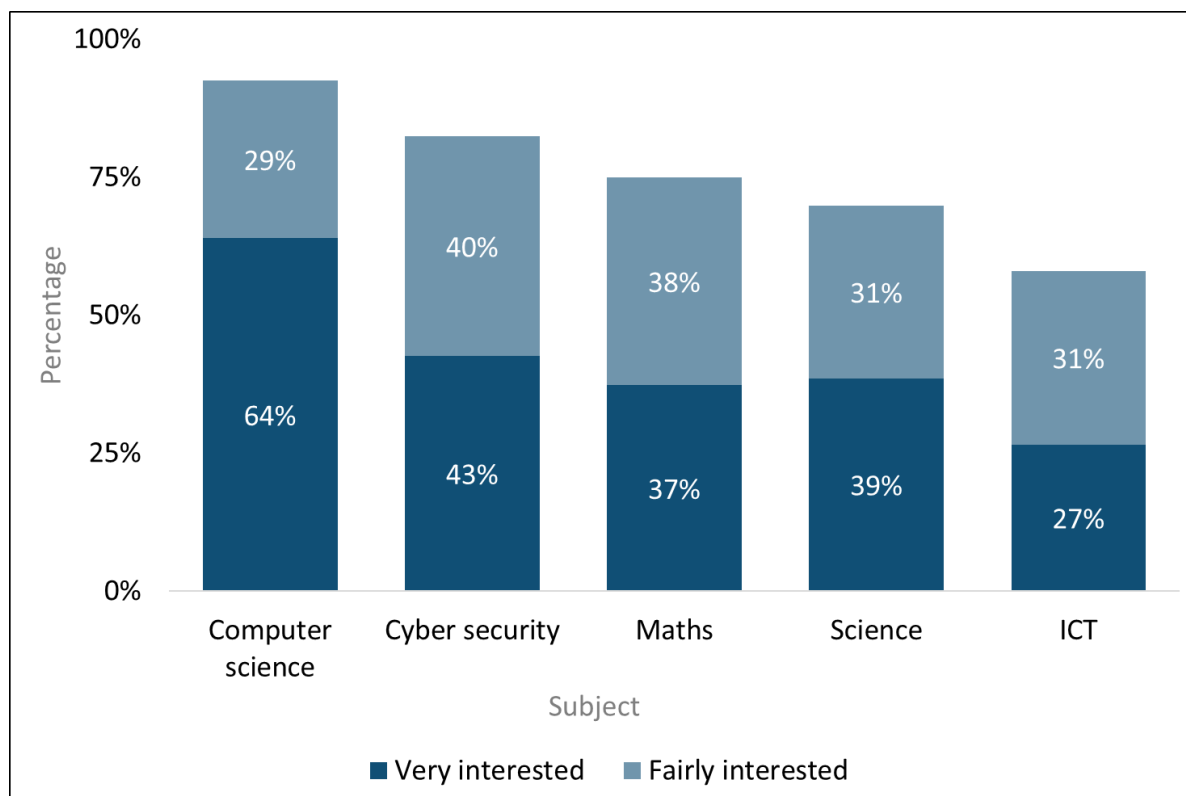
A higher proportion of respondents said they were very interested in studying computer science in the future (73%) than were very interested in studying cyber security (43%). Interviews suggested that this was because participants saw computer science as a broader subject and so there was more for them to be interested in. Around half were very interested in studying maths (53%) and science (46%), a higher level than seen for cyber security (43%). Smaller proportions were very interested in ICT (28%) and design and technology (12%).

These results show that Cyber Discovery is engaging participants who have a strong pre-existing interest in studying computer science. These participants are likely to have some relevant knowledge and skills, and may be the most talented students, which makes the programme more likely to achieve its objective of identifying the most talented.

Future career interest

The Year Three pre-survey also asked respondents how interested they were in careers involving certain subjects.

Figure 5: Future interest in careers involving subjects (Year Three)



Source: Year Three pre-survey. Base: 595.

The Year Three pre-survey asked respondents how interested they were in careers involving various subjects. Two-thirds of respondents were very interested in a career involving computer science, with a further 29% fairly interested. For cyber security, these figures were 43% and 40% respectively. This reflects a theme from interviews, that students often had a longstanding interest in computer science although, before taking part in Cyber Discovery, they had little awareness of cyber security. This may also reflect the fact that computer science classes were a popular recruitment channel for Club Leaders.

Future subject and career interest sub-group analysis

Male Cyber Discovery participants were significantly more likely to be interested in studying cyber security in the future (92%) than their female peers (81%). Male participants were also more likely to be interested in a future career involving cyber security (89%) than females (71%). This suggests that Cyber Discovery has successfully engaged girls despite them having lower existing interest in the subject than males albeit

that, as shown earlier, the proportion of girls taking part aged over 13 was generally slightly below 30%.

Whether respondents attended a state or private school did not impact their levels of interest in studying cyber security in the future or pursuing it as a career. There was also no difference in interest in either future cyber study or future cyber careers between white and ethnic minority respondents.

Participation in other programmes

Awareness

All those taking part in the Year Three pre-survey and Year Four single point survey were asked about their awareness and participation in other programmes and courses. These included specific cyber security courses (CyberFirst and Cyber Centurion) and more general courses. The following section covers Year Three pre-survey responses (full figures for Year Three and Year Four single point survey in Table 10 of Appendix Two).

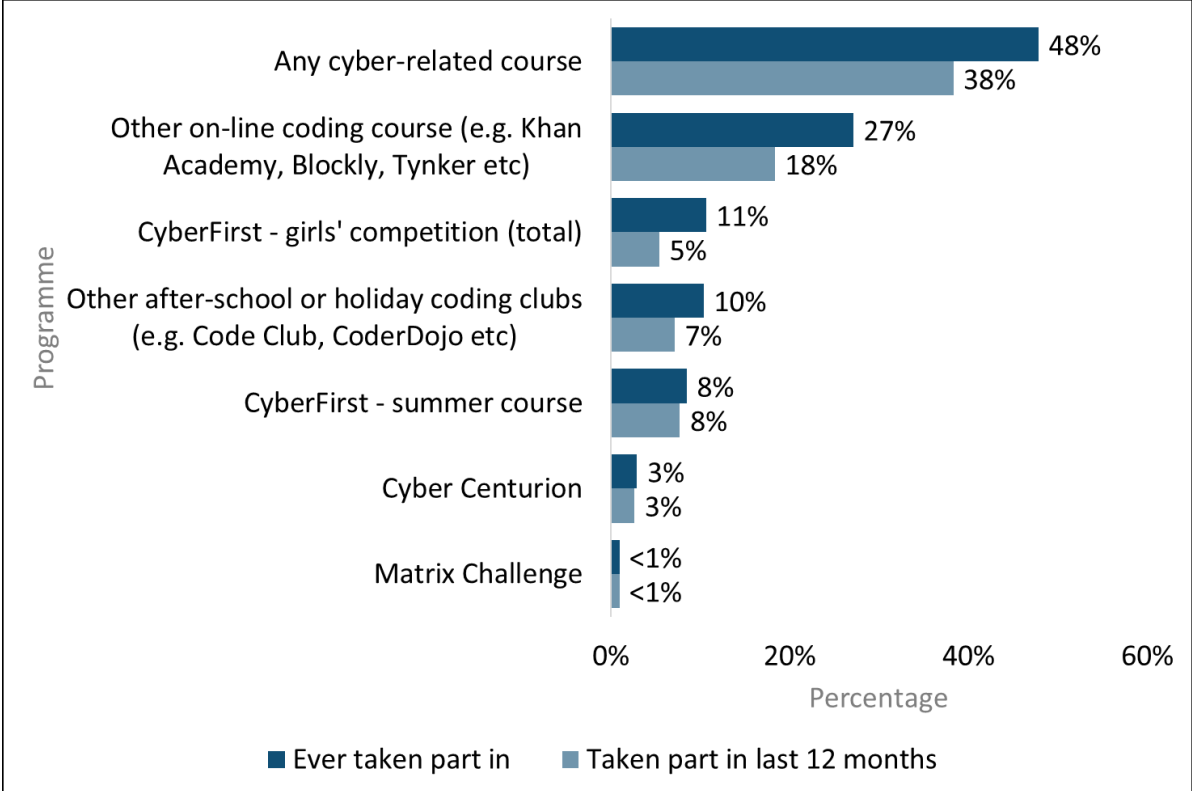
Responses at the Year Three pre-survey showed that around three-quarters (73%) of respondents had heard of at least one other programme, but that Cyber Discovery was reaching people who were not necessarily familiar with all the different cyber-related programmes. A third of all respondents (32%) had heard of the CyberFirst Girls' Competition, and for females this figure was 49%. More than a quarter had heard of the CyberFirst summer course (29%), and a fifth (22%) for Cyber Centurion.

Around half (52%) of all respondents had heard of other online coding courses (of which not all are cyber-specific). The other coding courses mentioned included picoCTF, Khan Academy, Immersive Labs, Cyber Security Challenge, Cypher Challenge, Codecademy, Bebras, Hack The Box, and the Alan Turing competition. Just over a quarter (28%) had heard of other after-school or holiday clubs, with Hack The Box being most frequently noted.

Recent and current participation

Results from the Year Three pre-survey showed that nearly half of Cyber Discovery participants had ever (48%) taken part in other programmes, with 38% doing so in the last 12 months, as shown in Figure 6 below.

Figure 6: Participation in Cyber Discovery and other programmes (Year Three)



Source: Year Three pre-survey. Q6. Base: 595.

There was a wide range of other programmes or courses that respondents had taken part in. Around a tenth of all Cyber Discovery respondents had taken part in the CyberFirst Summer Courses (8%) or the Girls’ Competition (11%), with the latter increasing to 28% among female only respondents. About a quarter (27%) had taken part in a different online coding course and 10% in an after-school or holiday coding course.

Future consideration

At the Year Three pre-survey, respondents were also asked which programmes they would be interested in taking part in. Most respondents (73%) said they would like to take part in at least one of the other programmes in future, with 24% interested in participating in CyberFirst Summer Courses and 13% in the Girls’ Competition (31% among females). Just under a fifth (17%) said likewise for Cyber Centurion, with 35% wanting to take part in another online coding course and 15% in other after-school or holiday coding club. These results suggest that participants were keeping options open at this stage and anticipating that they may want to be involved in other programmes in addition to their involvement in Cyber Discovery.

Understanding the cyber training marketplace

Many interviewees had been involved in CyberFirst, Cyber Centurion and Hack the Box as well as Cyber Discovery. They tended to be positive about Cyber Discovery in comparison, with this being largely expected as interviewees tended to be those who were most engaged in Cyber Discovery. Five main themes were identified:

- The gamification of the online stages made Cyber Discovery more fun and enjoyable than CyberFirst courses. Some students noted that this motivated them to progress through the stages and keep learning
- Participants felt they benefited from Cyber Discovery being open over a long period of time. They felt the experience allowed them to examine issues in-depth and could revisit content in their own time, therefore reinforcing their learning
- Cyber Discovery was felt to be more in-depth and covered a broader range of topics than other programmes. This helped students develop skills which they would not have learnt elsewhere, such as HTML and Python. This met the needs of students who were at the higher end of skills and knowledge

“Cyber Discovery is more immersive, it’s really engaging. Cyber Centurion is interesting...but it’s very long and can get repetitive. The difference with Cyber Discovery is that there are loads of different challenges that explore different concepts and ideas. That’s what makes it really interesting and makes you want to keep doing it.”

Student

- The increasing level of challenge and availability of guidance was felt to better suit the needs of students, than some more detailed initiatives. As an example, Hack the Box was perceived as a “big step up from Cyber Discovery”, which is understandable given the different programme aims (specifically the Hack the Box focus on professional pen testing)

“Cyber Discovery is perfect for beginners trying to get into it” *Student*

- Cyber Discovery was viewed as professional looking, user-friendly and appealing compared to other programmes

As noted, these themes represent the perceived strengths of Cyber Discovery among those who tended to be very engaged in the programme, hence it being unsurprising that they felt there were key strengths compared to alternative options.

Two potential areas for improvement were highlighted. One was that participants felt Cyber Centurion and CyberFirst Summer Courses allowed them to work with other students from other schools and that the long-running delivery period helped them build

online relationships. A separate theme was that some students who had not attempted Elite Camps felt CyberFirst provided more industry context than Cyber Discovery. These students said this helped them to “learn bigger picture stuff”, in particular content relating to real industry applications and to information on jobs using cyber security skills.

Reasons for participation in Cyber Discovery

The Cyber Discovery Theory of Change noted the importance of the Programme presenting a positive image so as to attract participants. In order to understand people’s perceptions of the programme, respondents were asked at the Year Three pre-survey and Year Four single point survey to say how much they agreed or disagreed with possible reasons for taking part in Cyber Discovery. This section focuses on results from Year Three, showing Year Four results as well where there were notable differences between the two years.

Results for Year Three suggested participants felt they were largely self-motivated as opposed to being encouraged to take part by others. Most pre-survey participants agreed strongly that they took part as they thought Cyber Discovery would be enjoyable (65%) or useful (51%) with most of the remainder stating they agreed (32% and 40% respectively).

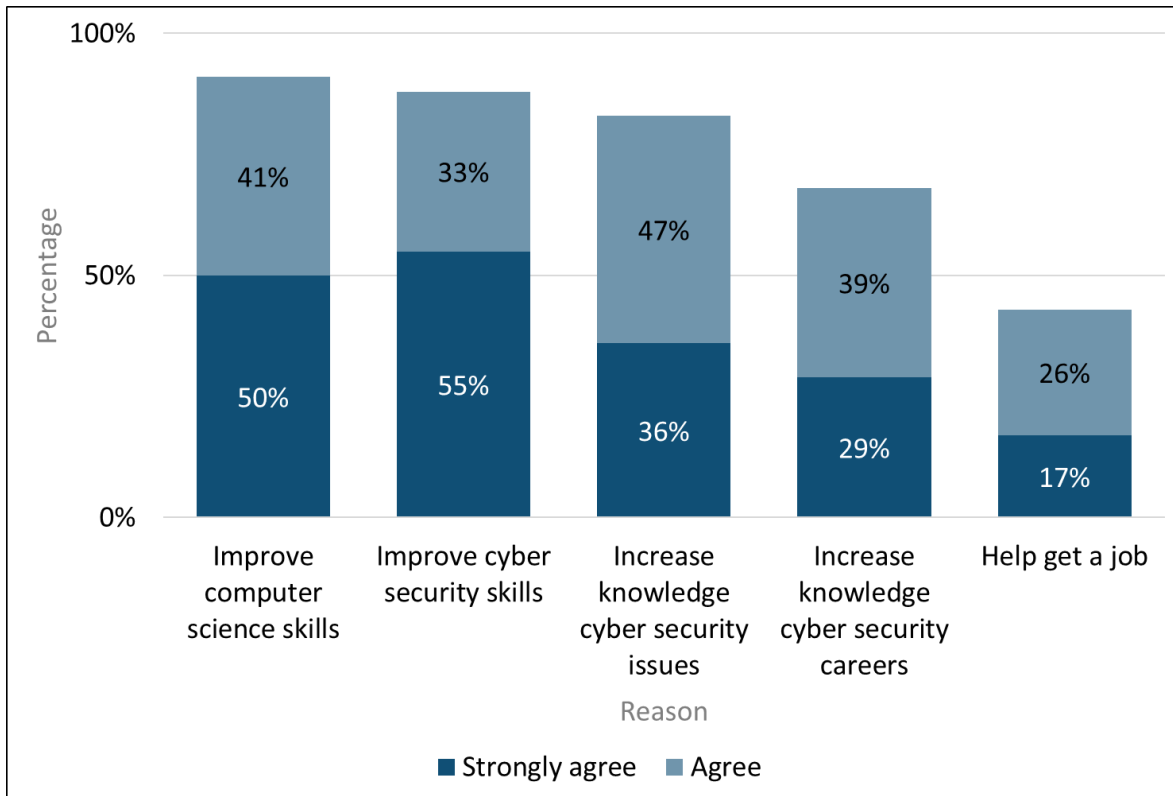
Teachers and friends were a particular influence for around a quarter, albeit with more generally agreeing (22% and 17% respectively) this was the case than agreeing strongly (8% and 6%). The proportions were lower in Year Four, with one in ten generally agreeing that teachers (9%) or friends (10%) were an influence, and only 4% and 2% respectively strongly agreeing. The lower influence from teachers and friends in Year Four may be due to COVID-19 restrictions.

At Year Three, relatively small proportions either agreed strongly or at all that they took part as their parents or carers wanted them to (1% and 8%) or as they had to take an extra-curricular activity (3% and 5%).

These findings suggest that participants had a genuine interest in the programme, rather than taking part solely out of a sense of obligation. This reflects positively on the way the programme was designed and marketed, with respondents generally viewing it as fun and informative.

The following figure shows the stated reasons for participation that related to skills, knowledge, or careers.

Figure 7: Reasons for participation: skills, knowledge, careers (Year Three)



Source: Year Three pre-survey. Base: 595.

Considerable proportions of participants took part in Cyber Discovery for reasons relating to skills, knowledge, and careers, linking with the high proportion seen earlier saying they were taking part as they felt it would be useful. Developing skills was particularly important, with large proportions taking part to improve their skills in computer science (50% agree strongly and 41% agree) or cyber security (55%, 33%). Smaller proportions agreed strongly (36%) that they wanted to increase their knowledge of cyber security issues although the overall proportions agreeing at all were at similar levels to the previous statements (47% agreeing in general). These findings show that participants' motivations for taking part broadly aligned with the programme objectives of increasing cyber skills and understanding.

Gaining knowledge around cyber security careers was a less important factor, although over half agreed strongly (29%) or agreed (39%) that it was a reason for taking part. Just under a fifth (17%) agreed strongly that they took part to help them get a job, with just over a quarter (26%) agreeing. This suggests that at least four in ten participants are at least partially viewing their involvement in the Programme in terms of job-related skills or content. Considerations around getting a job were no different for under-16 and over-16 respondents, suggesting older participants are not more motivated to take part by careers prospects.

At the Year Three survey there was little variation in reasons for taking part by age, with two exceptions. Under-16s (68%) were statistically more likely to strongly agree that they took part in Cyber Discovery because they thought it would be enjoyable, compared to over-16s (58%). Similarly, under-16s were more likely to strongly agree or agree (93%) that they took part to improve their skills in computer science, compared to 86% of over-16s.

Young people tended to think in interviews and focus groups about their reasons for taking part in two different ways. Firstly, there was a broad perspective that linked many of the reasons, seeing the programme generally as being interesting, fun and enjoyable and something that would give them the chance to look into an interesting subject. Secondly, there were those who also welcomed the practicality of the programme, noting the opportunity to gain hands-on experience. They tended to focus on the added value of the programme beyond what was in the curriculum and were very much more driven to participate by developing certain areas of skills and knowledge. In Year Four, several students highlighted that they were looking for something productive to do during lockdown, particularly where this could help with university or job applications.

Qualitative feedback also showed that while initial motivations may have been around enjoyment, this could lead to the training outcomes:

“I got more out of it than I hoped. I just wanted to do it for fun but I got three certifications from it. It’s gone beyond my expectations.”

Student

Club Leader participation

This section provides details on clubs and Club Leader participation, drawing on MI provided by SANS, interviews and data from the Club Leader survey where relevant.

Club Leader profile

MI data shows that roughly two-thirds of Club Leaders were men and a third were women. The majority were teachers, with parents and volunteers each accounting for small proportions.

Table 4: Club Leader status

Club Leaders were asked to record their status and gender at registration as part of the MI requirements. This showed:

	Year One	Year Two	Year Three	Year Four
Type				
Teacher	75%	87%	89%	87%
Parent	11%	6%	5%	5%
Volunteer	14%	7%	7%	8%
Gender				
Male	70%	64%	62%	62%
Female	30%	36%	38%	38%
<i>Base: Total sample</i>	<i>(1,341)</i>	<i>(1,881)</i>	<i>(2,099)</i>	<i>(1,572)</i>

Source: Management Information.

The actual number of Club Leaders increased from 1,341 in Year One to 2,099 in Year Three. This was largely due to increasing numbers of teachers taking part: teacher numbers nearly doubled from 1,010 in Year One to 1,859 in Year Three. There was a slight reduction in both the number and percentage of parents and volunteers each year. This was in part due to more stringent DBS checking requirements which increased the administrative burden for registering as a Club Leader, and also reflected the fact that marketing spend was largely focused on teachers.

Reasons for taking part

Club Leaders mentioned in interviews that they had various reasons for taking part, with these mainly focusing on benefits for the students such as developing cyber security skills or raising awareness of careers. One Club Leader said empowering students was important for their school as it was in an area of high deprivation. Cyber security provided a “pathway to success” for his participants, linking to other aspects of a cyber career path, including bursaries and apprenticeships. Another leader worked in an accredited CyberFirst school and explained that participation in Cyber Discovery helped them raise awareness of cyber security as a potential career option, particularly among female students and their families.

“Some parents wouldn’t think to suggest cyber as a career. The more parents and students can see it being available, then it becomes more normal as a conversation” *Club Leader*

Some leaders hoped Cyber Discovery would encourage participants to take computer science at GCSE or A-Level. A more minor theme was developing specific educational skills among students, such as programming and networking. Others hoped to encourage more general soft skills among students, such as independent learning and problem solving.

Leaders felt confident that the programme would benefit students and be easy to implement in their school. Knowing at the outset that the programme included resources such as the field manual reassured them they did not rely solely on their own knowledge or skills of cyber security to run the programme. They also felt more confident in the programme as it was backed by the government.

Club Leader activities

In Year Three, all Club Leaders who took part in the survey were asked to state which activities they had been involved in as a leader. Results are shown in the following table:

Table 5: Activities undertaken by Club Leaders

	Total
Encouraging students to sign-up to Cyber Discovery	97%
Providing assistance on Cyber Discovery challenges	84%
Providing advice on cyber security careers	67%
Raising awareness of the club among other staff members	67%
Arranging logistics (booking rooms, etc)	65%
Communicating with parents/carers about the Cyber Discovery club	42%
Other	3%
None	0%
<i>Base: Total sample</i>	<i>(69)</i>

Source: Club Leader survey. Q1.

All Club Leaders had taken part in at least one activity, with the vast majority (97%) being involved in encouraging sign-up, often targeting computer science students. Where Club Leaders adopted a whole-school approach, they tended to advertise the club to any student within the age limit first and then target specific groups, again primarily computer

science students. Channels included staff briefings, school websites, extra-curricular fairs and talking to students about the programme in lessons. This was often followed up with targeted conversations with students who teachers felt would particularly benefit, including females, potential computer science students or those who showed an aptitude for problem solving.

Over four-fifths (84%) of Club Leaders said they helped with challenges, with feedback suggesting this focused on the initial programme stages. One theme was that they tended to support students with the initial account set up, but then encouraged them to be self-reliant and resolve issues themselves or establish informal peer support networks. A separate theme was Club Leaders wanting to provide more and consistent support but occasionally finding certain content challenging or struggling to find the time to work out the answers to problems.

Two-thirds of leaders said they provided advice on careers (67%) or raised awareness of the club among staff (also 67%). Under half (42%) communicated about the club to parents and carers. Leaders tended to feel the programme was a “good sell” due to the professional looking website and government backing, noting that parents often asked how their children were progressing through the stages.

Industry expert participation

Industry interviewees had all supported Cyber Discovery by providing speakers and participants for events. One had also offered work placements to students. Industry experts took part to help with future recruitment, meet potential candidates, and raise awareness among participants of the range of roles available.

“The benefit of Cyber Discovery is that it's almost like talent scouting at the same time, so industry are getting something out of it too.”

Industry expert

A major theme was that experts saw their involvement as providing long-term sectoral benefits rather than immediate benefits to their organisation, primarily as students were unlikely to be immediately entering the job market. Experts were often involved as part of their organisational Corporate Social Responsibility (CSR) or from a more general desire to help the industry and inspire the next generation.

For industry experts working in smaller organisations, Cyber Discovery was an opportunity to showcase the industry without having to commit significant time and funds.

“SMEs [Small and Medium-sized Enterprises] don't have the capacity and ability to support structured work experience opportunities, so...the team are providing a way of giving them [students] exposure to businesses, to work

experience, to hands on experience outside of the home, outside of their bedrooms, outside of the standard day to day schooling life.” *Industry expert*

One industry expert also noted that they would not measure success in terms of numbers, but rather by the quality of candidates:

“It can't just be a numbers game. It's got to be about the results.”
Industry expert

Student intermediate outcomes

Summary

- Club Leaders and students found the platform engaging, user-friendly and intuitive
- Over three-quarters (84%) of Club Leaders said they provided guidance to participants, although interviews suggested they were not always able to do this consistently especially at more advanced stages
- Generally, students felt supported throughout the programme, albeit with some suggestions for additional guidance for less experienced students and individual participants
- Students who progressed found the level of challenge appropriate
- The majority of Club Leaders strongly agreed (62%) or agreed (32%) that Cyber Discovery provided young people with skills which they could not get through regular classes
- Club Leaders and curriculum experts were split as to whether Cyber Discovery needed to be explicitly linked to the curriculum. A common theme was that content enhanced the curriculum and met the needs of students seeking to broaden their knowledge and skills above what was already required in schools
- Interviews with previous participants suggested that participation in Cyber Discovery can help prepare students for higher education, through the development of relevant soft and technical skills
- Curriculum experts suggested the introduction of formal cyber security qualifications to meet the needs of students wishing to pursue this pathway
- Feedback compared to similar programmes was positive, feeling it was in-depth and fun compared to other programmes. Some students noted that social elements and industry context were stronger in other programmes

Functionality

Functionality refers to the user experience and platform design of the programme. As set out in the Theory of Change, functionality is the key requirement for effectively delivering content and keeping students engaged. Overall, students and Club Leaders felt the online platform function was designed well and provided support and guidance, although setting up virtual machines was sometimes difficult, and some wanted additional guidance.

Design and technical requirements

Several students and Club Leaders felt the interface of the programme was user-friendly and appealing:

“I really loved and enjoyed the programme. Really engaging, the challenges are well made, they’re really fun.” *Student*

“It’s been a really wonderful thing, there’s very little of any strand of computer science in other online challenges. Other things just aren’t as well managed and polished.” *Club Leader*

Some students identified technical issues as a barrier, for example not being able to install the original version of the virtual machines due to school or college security policies and processes. Often this could be overcome by students using their own personal computers at home, although not all students had this equipment, potentially those from families with less disposable income. This theme appeared to be more prominent in Year Four during school closures, particularly as students were participating at home more often and the platform performs more effectively using high-speed broadband.

“So, the very thing we were hoping to do, to encourage students from a fairly broad set of backgrounds to come and do this, was completely defeated by the use of the virtual machine.” *Club Leader*

These issues have since been addressed through upgrades to the Game technical infrastructure.

Support and guidance for students

Students were generally positive about the level of support they received, both from programme resources such as the field manual and from Club Leaders, although they did report that a degree of independent research was required. While data showed 84% of leaders helped students, feedback from interviews suggested that leaders did not always feel they were able to support students consistently. Leaders suggested some additional ways they could be better supported to help students through the programme:

- Information to help them directly signpost students to additional training or support when they are struggling
- Specific training sessions to outline the relevant skills required for students to complete challenges

- ‘Walkthrough’ sessions for Club Leaders and students to see an overview of the process before they start
- Clear information on progression criteria for progression to reduce potential discouragement if students are unsure why they had not qualified for stages
- An overall guide to Cyber Discovery, allowing Club Leaders to prepare for upcoming topics and provide details to students as required. This was also felt to be potentially beneficial in allowing them to plan links to the curriculum
- Development of an online community for Club Leaders, allowing them to share advice and tips on supporting students

Individual and club member students had slightly different perspectives on support and guidance, with individual participants being more likely to state they enjoyed working through the challenges on their own, whereas group members reflected on being positively motivated by working alongside peers. Despite this, individual members also felt it was helpful to talk through challenges with fellow students. Many had accessed informal online forums and raised the possibility of Cyber Discovery promoting an official moderated online forum or Discord Server incorporating hints and tips. Cyber Discovery does moderate a Discord server although it is less popular than the unofficial server,²³ suggesting that it might benefit from increased promotion or more content.

A minor theme was individual members tending to report a greater reliance on their own research or using the field manual. They felt the field manual was thorough, concise, accessible and student-friendly, comparing it positively to online articles they had found during independent research. The manual’s focus on skills development, rather than walkthrough solutions, helped them to build confidence during the early stages and learn how to approach similar challenges in the future. An additional minor theme was that the programme hint system which detracts points for using hints disadvantaged individual members, especially those with less prior experience of computer science or cyber security, as they are less likely to have a teacher or another student to ask for guidance. For some students, this affected motivation as they knew once they had used hints, there was no way for them to achieve full marks.

“I used hints a couple of times and they didn’t help at all, which was a bit disappointing as you lose points” *Student*

Image

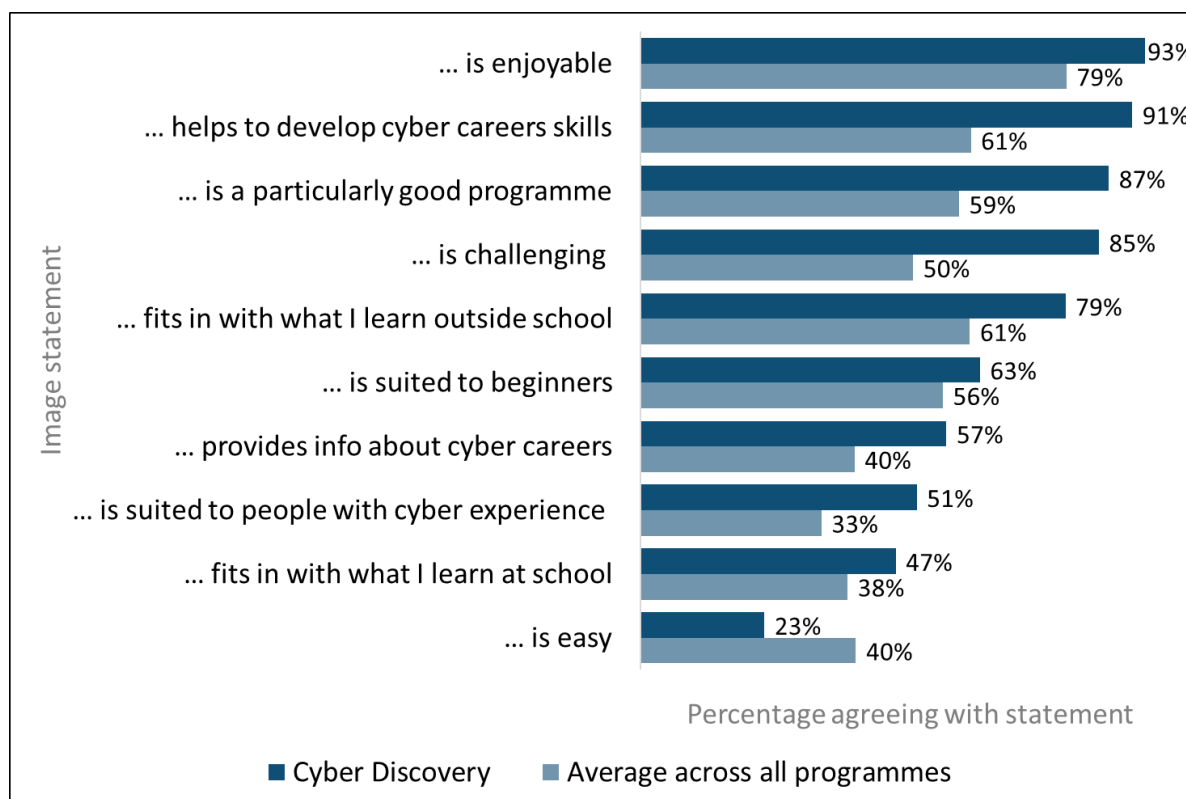
Ensuring that participants have a positive image of the programme helps encourage people to take part and helps Cyber Discovery stand out against competing programmes.

²³ <https://cyberdiscoverycommunity.uk/>

This section examines the image of Cyber Discovery and how it compares to other programmes.

At the Year Four single point survey, we asked respondents several questions on the image of other programmes they had taken part in, including CyberFirst. Figure 8 shows the proportion of respondents associating Cyber Discovery with each image and the average endorsement for other programmes.

Figure 8: Image of Cyber Discovery (Year Four)



Source: Year Four Single Point survey. Base: Cyber Discovery, 196; Average, 13-76 depending on programme.

Generally Cyber Discovery was endorsed at higher levels for each statement, as would be expected given that most respondents were actively taking part in the programme when they completed the survey. Comparison to the average programme allows us to assess the relative strengths of Cyber Discovery.

Provides right level of challenge

Respondents tended to feel that Cyber Discovery was challenging, with mixed views about whether it was well suited to beginners or people with cyber experience. In total, 85% of respondents felt that Cyber Discovery was challenging, much higher than the average across all programmes (50%). Conversely, about a quarter of respondents

(23%) felt that Cyber Discovery was easy, compared to 40% across the average programme.

Just over a quarter of respondents (29%) felt that Cyber Discovery was suited to *both* beginners *and* people with cyber experience, compared to 13% for the average across all programmes. There was no difference according to whether respondents had higher or lower self-reported cyber skills and knowledge. This suggests respondents felt that Cyber Discovery catered to people with varying levels of experience, more so than other programmes they had experienced.

Half of respondents (51%) felt that Cyber Discovery was suited to people with some experience, compared to a third (33%) across all programmes. Almost two-thirds of respondents (63%) felt that Cyber Discovery was well suited to beginners, similar to the average across all programmes of 56%.

Qualitative feedback supported the finding that Cyber Discovery was fairly challenging, at least relative to other programmes. A common theme was that having prior technical knowledge is beneficial, but not necessarily required if students are willing to invest time in researching solutions to problems and developing their skills. In addition, existing support and guidance, such as peer support and the field manual, were seen as useful tools to support beginners. A major theme was that participants welcomed the fact that Cyber Discovery was often difficult, enjoying the fact there were problems to solve.

A minor theme identified by Club Leaders was that the 'step up' from Assess to subsequent stages was steep for some beginners but overall, leaders reported that it was valuable for students to challenge themselves and develop soft skills such as perseverance and independent learning.

"There are others who haven't really thought of this kind of thing, they like sudokus and puzzles but haven't made the link between logic, maths and this [cyber security]. I think we find a lot of hidden talent through this...it grows their confidence." Club Leader

Enjoyable

The vast majority of respondents (93%) indicated that Cyber Discovery was enjoyable. This further suggests that the level of challenge provided did not detract from participant experience and may potentially have enhanced it.

Enjoyment of Cyber Discovery was high compared to the average programme respondents had taken part in (79%), especially to those outside of the CyberFirst portfolio. Out of those who had actually taken part in other courses, 99% felt that CyberFirst Girls Competition was enjoyable, while for Summer Courses this was 92%, for

Cyber Centurion it was 80%. About two-thirds of people felt that other online coding courses (66%) and after-school coding courses (69%) were enjoyable.

Links to extra-curricular training and learning

Over three-quarters of respondents (79%) felt that Cyber Discovery fitted well with what they learnt outside of school, for instance in other courses or their own study. This compared to 61% across all programmes, 73% for CyberFirst Summer Courses, and 61% for other online courses.

Links to the curriculum

Roughly half of respondents (47%) felt that Cyber Discovery fitted well with what they learnt at school, compared to an average of 38% across all programmes. Year Four interviews and focus groups focused on links to the curriculum and how much this should be an aspiration of the programme. A strong theme from interviews with Club Leaders and students was that links to the curriculum were limited but this was because Cyber Discovery went far beyond the content covered in the classroom. For many, this was a strength of the programme as students enjoyed developing skills and knowledge that they had not had the opportunity to discover previously.

“I think it’s ahead of school in the way it’s able to teach people those skills. Computer science is under prominent in school...Because the world is moving into a more technological era, it’s important that there are people equipped with the skills to keep people safe online. That’s what makes Cyber Discovery really useful to have under your belt.”

Year Four student

Others felt Cyber Discovery complemented GCSE and A Level computer science, with some students saying that the content they learned in Cyber Discovery gave them a better understanding of topics they were studying in school or college, for example definitions of malware and some low-level programming languages like assembly. One student noted that his prior experience through Cyber Discovery put him at an advantage in his GCSE Computer Science class compared to peers who had not participated.

“Things I’ve been learning there [in Essentials], I’m only just covering now so I’m miles ahead of my classmates.” *Year Four student*

In addition, follow up interviews with students who are now studying related degrees at university suggest that participation in Cyber Discovery could help prepare students for higher education.

“[Cyber Discovery] is leagues above what you do at degree level. I’m in second year [of a forensics, computing and security degree] and it’s so much better. A lot of people lack the basic skills, so you’re sat there trying to help them. If they’d done a programme like Cyber Discovery it would have massively helped them with their degree.”

Year Four student

In addition to the relevant technical skills and knowledge gained through Cyber Discovery, a major theme was that the programme provides valuable real life context about what students are learning in the classroom. Some Club Leaders and students acknowledged that it would be difficult to incorporate this aspect into formal qualifications as it requires a different style of learning.

“It’s really unique, really different to learning in a classroom where you write stuff down and remember it. It gives you the experience first-hand, a really effective way to learn it. I don’t think you could emulate that in a school environment. This is a once in a lifetime opportunity.” *Year Four student*

Club Leaders provided several views on whether programmes like Cyber Discovery should strive to introduce more links to the curriculum. A major theme was that this could potentially make them less fun and appealing to students. Some felt that explicitly linking the programme to the curriculum could be detrimental. Firstly, it was noted that this could detract from independent learning and research, with some seeing this as an important skill that students developed through Cyber Discovery. A further theme was that too much emphasis on links to computer science curricula could have a negative impact on diversity, as it could deter students from other disciplines, such as maths, from taking part.

An alternative view was that having links to relevant computing curricula could benefit less confident students. One Club Leader noted that some students sometimes felt daunted by unfamiliar content, deterring them from continuing with the programme.

“I think having links to the curriculum is really helpful. It can then go further but needs that basic link. Then at least the students have that idea, ‘I understand that. It’s not new to me’.” *Club Leader*

Interviews with curriculum experts suggested that four key decision makers or stakeholders were important when considering curriculum links in school; computer science departments, maths departments, head teachers and careers staff. The table below summarises the major themes relating to each role and highlights the range of aspects to consider in relation to introducing links to the curriculum.

	Computer Science Departments	Maths Departments	Head Teachers	Careers Staff
Reasons for introducing initiatives	<ul style="list-style-type: none"> To encourage students to choose GCSE or A-Level Computer Science, by showcasing enjoyable elements of the subject and interesting potential career pathways To nurture an interest in the subject and highlight potential future pathways 	<ul style="list-style-type: none"> To develop problem solving and logical thinking skills To demonstrate that you don't need a computer science degree to pursue a cyber security career (for example raising awareness of apprenticeships) 	<ul style="list-style-type: none"> To support STEM, offer extra-curricular activities, and provide career information To showcase the school to parents and prospective students 	<ul style="list-style-type: none"> To access and signpost information and resources relating to career pathways from one location
Importance of curriculum links	<ul style="list-style-type: none"> A strong theme that some links are beneficial, but supplemented by additional content which goes beyond it 	<ul style="list-style-type: none"> Specific links to the curriculum not necessary (although does link to cryptography at KS3), but the soft skills developed are relevant to maths 	n/a	n/a

<p>Additional observations</p>	<ul style="list-style-type: none"> • Some suggested they would like to see a standalone Cyber Security qualification. One noted this would particularly appeal to female students, who are often put off by the programming-heavy content of computer science courses 	<ul style="list-style-type: none"> • Interested in developing a STEM curriculum that runs through the school. Would like to see 'unplugged' resources relating to cryptography to encourage creative thinking about how to crack a code or solve a puzzle, criticality, computational thinking 	<ul style="list-style-type: none"> • For a school with high proportion receiving pupil premium, the key is motivating students to aim high and step outside their comfort zone 	<ul style="list-style-type: none"> • Important that all staff are aware of cyber career pathways as they influence students' choices
---------------------------------------	--	---	---	---

Student outcomes

The Theory of Change includes Cyber Discovery outcomes covering cyber security interest, education and training; cyber careers; and a programmatic outcome to include a range of participants. By building participant interest in cyber, encouraging future study and careers, identifying the most talented, and engaging underrepresented groups, the programme aims to achieve its intended impact. This chapter examines each of these in turn.

Cyber security

Interest, knowledge and skills

Knowledge and skills

All respondents were asked at the Year Three pre and post-survey to state how they would rate aspects of their knowledge and skills using a scale from zero (very poor) to ten (very good).

Table 6: Knowledge and skills ratings (Year Three)

	Mean		Pre-post Change
	Pre	Post	
Skills in cyber security	5.7	7.0	1.2
Skills in computer science in general	7.3	8.1	0.8*
Knowledge of cyber security issues, for example cracking codes, fixing security flaws etc	6.4	6.9	0.5
Ability to solve problems	7.8	8.1	0.3
Skills in Maths	8.1	8.3	0.2
<i>Base: Total sample</i>	<i>(115)</i>	<i>(115)</i>	<i>(115)</i>

* indicates statistically significant change.

Source: Student Year Three pre-survey. Q8. Student Year Three post-survey Q8.

Results in Table 6 show that the programme contributed to increasing technical cyber and computer science skills. Respondents reported a statistically significant increase in their skills in cyber security (5.7 to 7.0) and in computer science (7.3 to 8.1), although knowledge of cyber security issues did not show any significant change (6.4 to 6.9).

Students felt proud of their improved skills and linked this to the challenging nature of the programme:

“My skills have increased at least three-fold. My skill level is now far better than people my age.” *Year Three GIAC student*

Students who had progressed through the course said they now knew more about programming languages such as Python, HTML, ciphers, steganography (hiding secret messages in ordinary communication), terminal activities, infrastructure networks and the dangers of poorly designed software. One Club Leader noted that, since taking part in Cyber Discovery, students were able to use more technical wording, helping them to better understand their course content. Several students highlighted that they particularly valued the opportunity to gain hands on experience relating to real life scenarios, such as the Hack-A-Bot activity at Elite Camp.

People studying cyber-related subjects at university and had taken part in Cyber Discovery previously reported in interviews that the programme helped them to develop a breadth of knowledge that they would not have gained otherwise.

“It’s definitely given me that knowledge that I can cover all categories, not just the offensive, I’ve attended talks about the forensics side, going into tools and techniques. It helped me become a good all-rounder, showed me the different areas of cyber security available to me.” *Long-term follow-up student*

Industry experts reflected on the general high-level of skills and knowledge shown by Cyber Discovery participants. One reflected positively on the skills and approach shown by an apprentice who had taken part in the programme:

“We’ve had conversations with them about incident response. They want to work in a role where they fix those problems. It shows they’ve been equipped with the knowledge and are being active, having conversations with employers. This is one way we’ve seen an increased awareness as a result [of Cyber Discovery].” *Industry expert*

Overall interest in cyber security and computer science

Year Three data showed that respondents’ self-reported interest did not change from pre to post-surveys for either computer science (8.8 at pre and post) or cyber security (8.1 and 8.2). One possible explanation for the lack of change in interest is that it was already high at the pre-survey. It is unlikely that everyone would ever rate their interest at 10 out of 10, so we would not expect means to increase much beyond 8 or 9.

Qualitative information suggested that where interest may have increased that this was due to a particular improvement in skills development. One student described how learning about updating websites increased their interest in this area and encouraged them to carry out further independent learning about vulnerability in web browsers. Interviews suggested that the programme was particularly engaging for some students with a longstanding interest in computing and technology.

“It opened my eyes to the exploit development aspect [of cyber security]. I've loved it so much I've gone away and done my own research. It's definitely spurred me on to learn. I now teach and mentor people about exploit development. It's an area I never would have thought of. You see hackers in movies bashing away at a keyboard, you don't see what actually goes on. This is one of the areas that isn't seen or heard of.” *Year Four Student*

Curricular uptake

Students were asked in the Year Three pre-survey to state their interest in studying certain subjects at the start of the academic year, and at the post stage their current level of interest in the same subjects.

Table 7: Percentage very interested in studying each subject in future (Year Three)

	Pre	Post	Change ²⁴
Maths	45%	46%	+1%
ICT	28%	29%	+1%
Design and Technology	8%	9%	+1%
Science (e.g. biology, chemistry, physics etc)	36%	35%	0%
Computer science	69%	62%	-6%
Cyber security	61%	48%	-13%
<i>Base: Total sample</i>	<i>(115)</i>	<i>(115)</i>	

Source: Student Year Three pre-survey. Q10. Student Year Three post-survey Q13.

²⁴ Change is calculated prior to rounding pre and post figures, so does not always correspond exactly to change observed between rounded figures.

Overall levels of endorsement were high for most options, with respondents on average stating that they were very interested in more than two different subjects at pre-stage and post-stage. This indicates that those taking part throughout Cyber Discovery may be 'very interested' in studying a specific subject, but it is not necessarily the sole focus of their interest and that broad interest across subjects has not changed from pre to post stage.

There was no statistically significant change in the percentage of respondents who were very interested in studying cyber security decreased between pre (61%) and post (48%) survey. The percentage who were not very interested in studying cyber security stayed at similar levels (14% and 12%), with no respondents stating that they were not at all interested at either stage.

The proportion who were very interested in computer science stayed at similar levels from pre (69%) to post (62%), as did endorsement for other subjects, suggesting that the decrease for cyber security was not due to a general decline in interest for similar subjects.

At the Year Four single point survey, nearly three-quarters of respondents (73%) said that they were more likely to study cyber security at university as a result of taking part in Cyber Discovery, with 64% saying they were more likely to study computing. Therefore, while prepost data suggests that there is no change in future interest in studying cyber security or computer science, participants nevertheless perceived that Cyber Discovery had a positive impact on their likelihood of future study. However, increased consideration in these university options will not necessarily translate into respondents actually applying for or studying these courses, and there may be other subjects that respondents prioritise more highly.

Future training uptake

Year Four survey respondents were asked whether Cyber Discovery made them more or less likely to take part in CyberFirst activities and other cyber security training. Four out of five respondents said that they were much more likely (47%) or somewhat more likely (36%) to take part in other cyber security training. A further 15% said their likelihood was about the same as a result of Cyber Discovery, and 2% said it had decreased. For CyberFirst activities specifically, two-thirds said they were more likely to take part, with roughly a third selecting each of 5 (33%), 4 (35%), and 3 (30%) on the five-point scale.

These figures show that Cyber Discovery is effective at building interest, possibly reflecting general enjoyment of the programme. There is also evidence of Cyber Discovery fitting into the CyberFirst pipeline, with more than two-thirds of respondents saying they were more likely to take part in CyberFirst activities as a result of the programme.

Awareness of future education or training options

At the Year Three post-survey, most respondents were aware of further education or training opportunities. Around four-fifths had heard of Cyber Security degrees (82%) or apprenticeships (81%). Awareness of recognised cyber security certificates (for example, the Certified Ethical Hacker certificate) was at 69%, with half (50%) having heard of cyber security bursaries and 44% being aware of other educational or training opportunities. Since this question was only asked at the post-survey, it cannot tell us whether Cyber Discovery increased awareness of different education and training options. However, the fact that awareness was still relatively low for certain non-university pathways, such as professional certification and cyber security bursaries, suggests that Cyber Discovery could do more to communicate different options to participants.

Cyber security careers

This section provides detail on Club Leader perceptions of careers and online platforms, followed by similar information from students.

Results show that participants reported receiving information from Cyber Discovery on careers albeit not more than from other programmes and as one of many sources of career information. Among all participants, understanding and knowledge of cyber careers increased over the time participants took part, but their view of the importance of cyber security or the availability of careers remained at similar levels. There was no evidence that participants were more likely to consider careers in cyber security after having taken part in the programme.

Interview feedback suggested that participants at Elite Camp received more career information and welcomed this detail. Club Leaders also felt that they did not necessarily have access to relevant careers information either in or out of school.

Student overall career perceptions

This section includes students' interest in specific career options, cyber security career information sources, their perception of cyber security careers and knowledge of the requirements to pursue a career in this field.

Cyber security career information sources

When asked in the Year Three post-survey, virtually all (95%) those who took part in Cyber Discovery felt it provided them with at least some information on cyber security as a career.

Over half of respondents had accessed information on cyber careers from academic study or teachers (59%), other similar courses or cyber security programmes (54%), or

online resources (51%). More traditional sources of careers information were also highlighted, with 44% having received information from open days or careers fairs and 41% from careers advice services. Friends and parents or family members had each acted as sources of cyber careers information for 40% of respondents, and social media (43%) was a more cited source of information than regular media (23%). This suggests that Cyber Discovery is an important source of information for participants, but that there is a broad range of other sources.

Cyber Discovery participants felt the amount of career information provided was similar to what they received from other programmes. At the Year Four single point survey, respondents were asked to indicate which programmes, out of all that they had heard of, provided lots of information about cyber security careers. Over half of respondents (57%) felt that Cyber Discovery provided lots of information, compared to an average of 50% across all programmes. Almost all who took part in the CyberFirst Summer Courses (89%) felt it provided a lot of information on careers.

A key theme in interviews was that the most detailed Cyber Discovery career information was mainly provided at the Elite stage. The level and quality of information provided was appreciated, albeit with a minor theme being some wanting additional information or exposure to a wider range of sectors. Interviewees reflected positively on industry talks, the opportunity to meet industry experts and being provided with a book outlining the different routes into the industry.

Some students recognised careers information had been provided at early stages in the programme and that this was useful. A common suggestion in Year Three was that more detailed information should be incorporated throughout the programme so that all students were aware of the next steps to pursue a career in cyber security, thereby benefiting all participants as well as the most talented:

“I wouldn’t say they were well defined next steps, I don’t know about people who’ve done Elite [who have more opportunity to meet people in industry] but just generally in the course, there’s not much about what you can do afterwards. Even if it’s just a page of useful links to learn more would be really good.” *Year Four student*

Several students suggested that there should be a programme that could collate relevant careers information (for example, information on apprenticeships, bursaries, the showcasing of different roles) into one resource so they could keep track of deadlines and reduce the time spent researching opportunities. It was suggested that additional information could be incorporated into Cyber Discovery, such as a separate module on careers guidance or a dedicated web page.

Perception of cyber security

At the Year Three pre and post-surveys, respondents were asked to state the extent that they agreed or disagreed with a set of statements about understanding cyber.²⁵ Results suggested that over the time they were involved in Cyber Discovery, participants were more likely to agree strongly that cyber security was very important to society in general (51% to 68%), but they were no more likely to say cyber was important for their career (44% to 46%) or for everyday life (35% to 30%).

Perception of cyber security careers

All respondents were asked to state their understanding and knowledge about cyber job roles at both pre and post stages, using a scale from zero to ten.

Table 8: Knowledge and understanding ratings (Year Three)

	Pre	Post	Change
Understanding of different cyber security job roles	5.8	6.8	1.0*
Knowledge about careers in cyber security	6.0	6.8	0.8*
<i>Base: Total sample</i>	<i>(115)</i>	<i>(115)</i>	<i>(115)</i>

* indicates statistically significant change.

Source: Year Three Student pre-survey Q8. Year Three Student post-survey Q8.

There was a positive change in Cyber Discovery participants saying that they had a good understanding of different cyber security job roles (from 5.8 at pre to 6.8 at post), while knowledge about careers in cyber security was 6.0 and 6.8 at the same time periods.

Respondents associated these positive changes with their involvement in the programme. Over three-quarters agreed strongly (24%) or agreed (60%) that Cyber Discovery helped them develop skills to pursue a cyber security career. Around two-thirds of respondents agreed strongly (31%) or agreed (34%) that it helped them know what steps to take to pursue a cyber security career.

Respondents felt they generally knew enough about cyber security career requirements. Around two-thirds to three-quarters either agreed strongly or agreed that they knew about the required skills (23% agreeing strongly, 52% agreeing), study requirements (22%, 49% respectively) and information sources (23%, 45%). Just over half felt they knew

²⁵ This question uses identical statement wording in relation to science used in the [2019 Science Education Tracker Wave 2](#), *Young People's Views on Science Education*. Questions were asked of a nationally representative sample of Year 7 to 13 students in England about science.

enough about the actual steps that were required to get a cyber career (18%, 43%). The lower relative proportion who agreed strongly links with the earlier overall rating of knowledge at the post-stage (6.8) – participants say they know more about cyber careers than previously and have a solid understanding, but that there is more they could know.

The gap in overall knowledge is backed up by Year Three post-survey data on whether respondents felt that they knew enough about cyber security to know if it was a career option for them. When asked if they *didn't* know enough, 23% disagreed strongly that they didn't know enough, with 40% in total disagreeing, suggesting that about two-thirds of people felt they did know enough to assess it as a career option. There was a notable minority that did not disagree, with just under a fifth (18%) agreeing or disagreeing, and a similar proportion either agreeing strongly that they didn't know enough (6%) or agreeing (13%).

Feedback from students and Club Leaders in interviews suggested those who received careers information from Cyber Discovery felt it made a difference:

“The fact I've learnt a lot more about career paths, what it's like to work in the cyber industry, I think that's one of the main reasons I've applied [for a cyber security degree].” *Year Four student*

Those who had progressed relatively far in the programme tended to reflect positively on the careers information, feeling it gave them a better understanding of the variety of career options relating to cyber security and more information about the next steps to pursue a career in the sector. Some students noted that they had limited awareness of opportunities relating to cyber security and Cyber Discovery helped confirm that it was what they wanted to do.

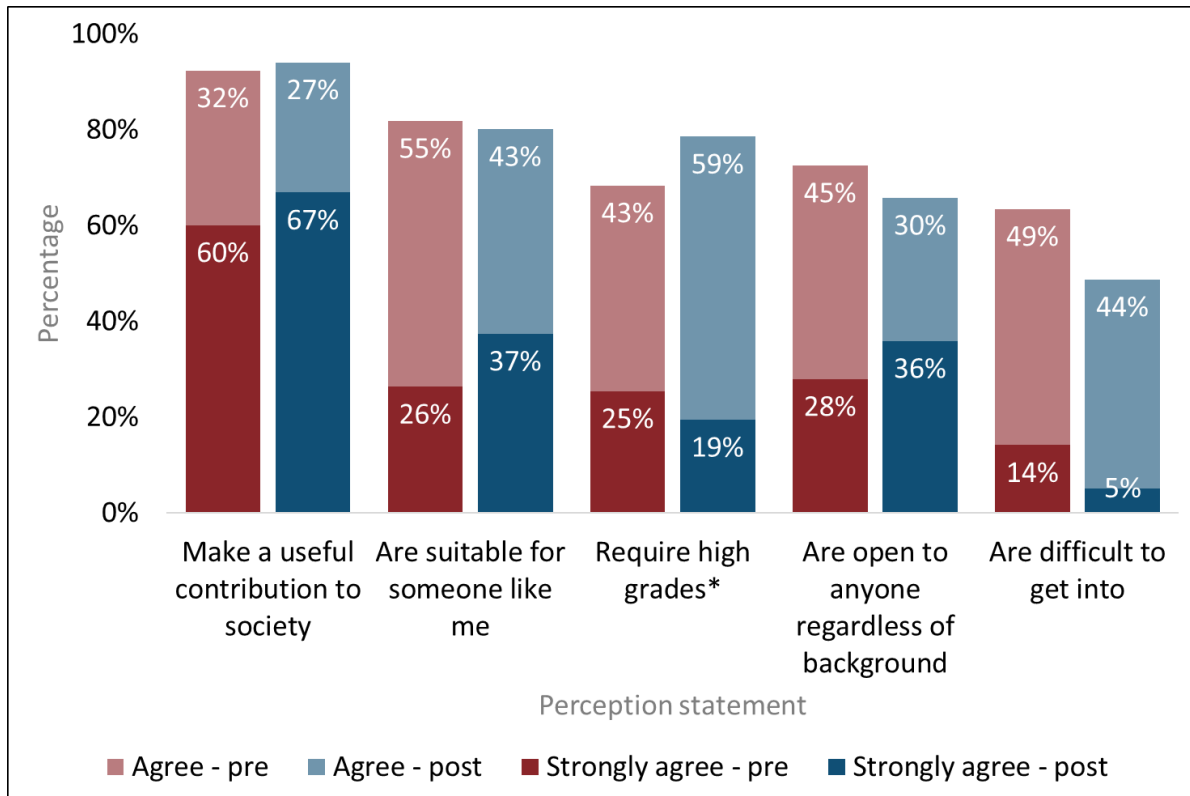
“Cyber Discovery has really helped me think about how I want to do it more. I already had an idea but Cyber Discovery has made that idea certain.” *Year Four student*

“Originally I was not looking into a career, but since starting and realising the skills I'd need, I've realised how interested I am and want to do it as a career and university course. [Without Cyber Discovery] I wouldn't have known how much I enjoy it.” *Year four student*

Cyber career relevance and availability

All survey respondents were asked how much they agreed or disagreed with certain statements about the potential relevance or availability of cyber careers.

Figure 9: Perception of cyber security careers (Year Three)



* indicates that change in all agree is statistically significant

Source: Year Three pre-survey. Q12. Year Three post-survey. Q20. Base: 115.

While respondents felt they received some career information from Cyber Discovery and their knowledge and understanding of job roles had increased, they did not necessarily see cyber jobs as more relevant or available. Perceptions, however, were generally positive at the pre-questionnaire and remained so at the post-stage. The sole exception was that the proportion agreeing that cyber careers require high grades increased from 68% to 78%.

Although there was no change over time, participants generally had a very positive view of cyber careers. Information from the Year Three post-survey and Year Four survey (data is from Year Three unless stated otherwise) showed that:

- Most participants felt cyber careers made a useful contribution to society (94% agreeing), a similar level to the proportion noted earlier who felt understanding cyber security in general was important for society
- Respondents also felt that cyber careers were generally accessible, with around three-quarters of respondents agreeing that cyber security careers were suitable for someone like them (80%), and two-thirds that cyber security careers were open to anyone regardless of background (66%). Almost all agreed cyber careers were

open to everyone regardless of ethnicity (88%, Year Four). About half (49%, 5% strongly, 44% agreeing) felt that a cyber career was difficult to get into

- Most respondents disagreed (72%) that it was more suited for men than women, with male and female participants having similar views.
- The general perception was that cyber careers required high grades (78% agreeing), and that it paid particularly good salaries (79% Year Four)
- Participants generally disagreed that a career in cyber would be boring (85% disagreeing)

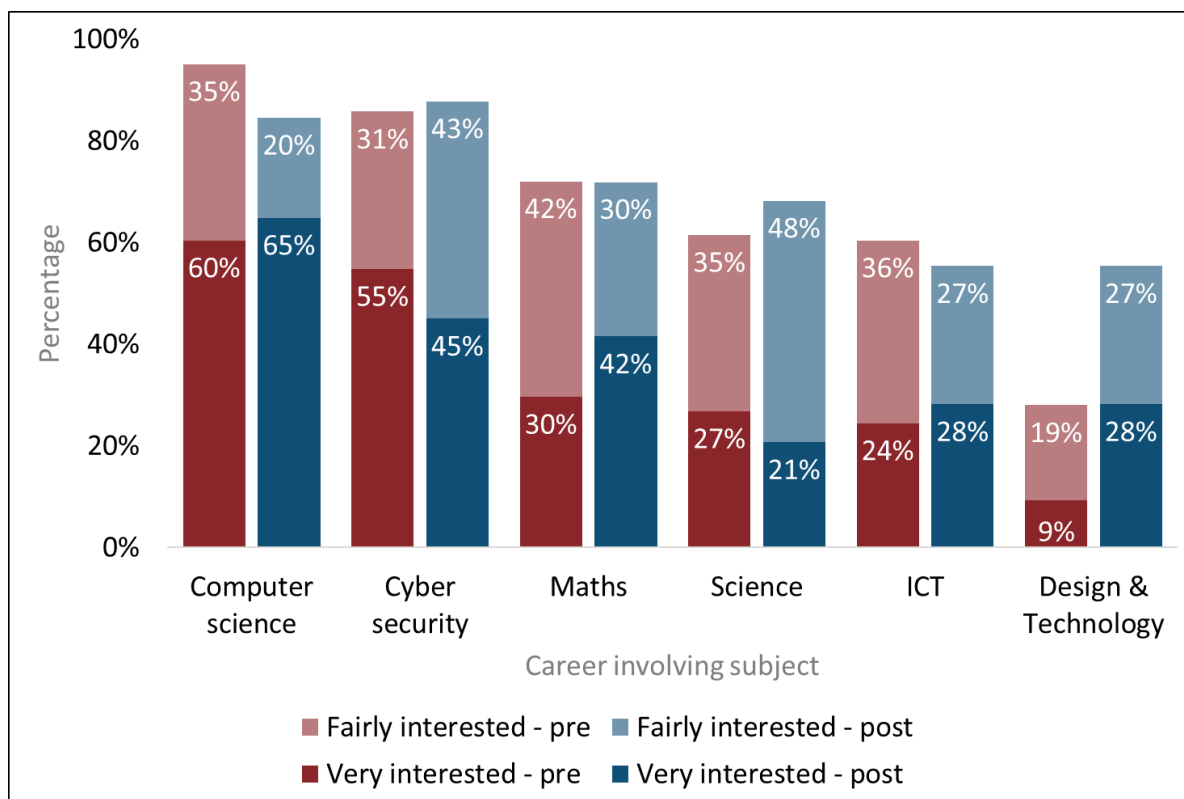
Participants were less sure at Year Four about whether cyber careers were only for people who are good at technical things: 35% either agreed strongly or agreed, 29% neither agreed or disagreed, and 36% disagreed. They also tended to agree in Year Four that cyber careers were not well promoted (47% agreeing, 32% neither agreeing or disagreeing, 21% disagreeing). Respondents felt that cyber careers paid good salaries: 79% agreed strongly or agreed, compared to 19% who neither agreed nor disagreed and 2% who disagreed. Finally, there was strong agreement that cyber careers are open to all regardless of their ethnicity. Over half (53%) strongly agreed, with a further 35% agreeing. There was no difference in level of agreement for white and ethnic minority respondents. Only 2% disagreed, with 10% neither agreeing nor disagreeing.

More broadly, Year Three post-survey data showed that respondents were generally open to careers that fitted cyber security skills and also other skill sets. Highest levels of being very or fairly interested in careers related to those involving problem solving (100%) and critical thinking (97%), suggesting a specific interest in careers requiring broad analytic skills. More general soft-skills were endorsed by most respondents but at a lower level than more analytical skills, including working on their own (82%) or in teams (77%), with similar proportions interested in careers involving organisational skills (79%). Around two-thirds were interested in careers involving oral or spoken communication (66%) and about half with written communication (47%), with most of those who were interested in those careers being fairly rather than very interested in them.

Career interest by subject

The Year Three pre and post-surveys were designed to measure longer term changes in career interest for different subjects. At pre-stage they were asked to state their interest at the start of the academic year, and at post-stage their level of interest at that time.

Figure 10: Very and fairly interested in career involving each subject (Year Three)



Source: Year Three pre-survey. Q11. Year Three post-survey. Q13. Base: 115.

None of the changes from pre to post were statistically significant, both in terms of percentages who were very interested and percentages who were either fairly or very interested. Interest in careers involving computer science was high (95% and 85%), as was interest in cyber security (81% and 88%).

Data from the Year Four single point survey showed half of all respondents (49%) felt Cyber Discovery made them much more likely to consider a future career in cyber security, and a further 37% said that they were somewhat more likely. A further 13% said that their likelihood of considering a cyber career was about the same as a result of taking part in Cyber Discovery, and 1% felt that they were less likely. As with similar single point in time questions, this may well reflect the fact participants enjoyed taking part in the programme. Results for this question on consideration should be seen in the context of the earlier Year Three results showing no pre to post increase in interest in cyber careers.

It is possible that results among the Year Three pre and post-sample are not representative of the total population taking part in Cyber Discovery (see “data limitations” section), particularly given the relatively low base size for this question. It is likely that factors outside of the Cyber Discovery programme have also affected interest,

including other courses and advice from teachers and family members. This makes it difficult to contribute any increase or decrease in career consideration to the programme.

Data from across the Theory of Change provides valuable contextual information for the change in career consideration. Comparison of pre and post data showed an increase in skills in cyber security and the understanding of job roles and careers. The vast majority of respondents felt that Cyber Discovery provided them with information on careers and that the programme gave them required careers skills and knowledge about the next steps, albeit that they are still interested in a variety of other career options.

One hypothesis consistent with the tentative evidence to date is that Cyber Discovery may have made some young people aware of the actual nature or requirements of a career that they may not otherwise have known about. This may have made some participants shift from being “very” to “fairly” interested. This fits with evidence suggesting that participants are interested in a variety of different subjects and careers at this stage and with some qualitative feedback that the programme provided them with a realistic picture of what is required:

“It’s definitely given me an insight into what the job would be like. I’ve always had a bit of an interest in computer science but not really considered it as a job.” *Year four student*

While this fits with the balance of evidence across the Theory of Change, this remains a hypothesis with other explanations also being possible. It may be, for example, that there are other reasons not related to Cyber Discovery as to why career consideration may have decreased or that the programme has not worked as intended for some. It may also be that knowledge and skills gained on cyber security have not kept pace with knowledge and skills about other subjects from other sources, hence no increased interest in cyber.

It is also important that 88% of Cyber Discovery participants stated at the Year Three post-survey that they were very or fairly interested in a career in cyber security, given the programme’s objective to fill the existing cyber skills gap. However, it is unlikely that all of those who say they are very or fairly interested will progress into actually applying for relevant jobs, so this 88% figure will likely translate into much lower actual cyber career uptake.

There is economic evidence highlighting the importance of increasing interest and take-up of cyber security careers. Evidence shows that a male computing graduate is expected to earn £10,995 more than the average male graduate over a ten-year period, while a female will earn £3,774 more²⁶. This shows the possible monetary impact of Cyber Discovery students taking up a career in cyber security but should not be linked to

²⁶ [DCMS \(2020\) Cyber security skills in the UK labour market](#)

the earlier data on career consideration (namely assuming the decrease in career consideration suggests a negative financial impact). This is not least due to the length of time until survey respondents actually move into careers, the changing nature of the cyber job market, and the lack of counterfactual information to assess what may have happened had respondents not taken part in the programme. There may be other financial benefits through broader upskilling leading to increased safety from cyber threats in general and/or skills gained leading to improved financial benefits in other, non-cyber careers. Students and employers may also benefit from students deciding a career in cyber security is not right for them, allowing a better match between students and employers.

Club Leader and careers

The Year Three Club Leader mini survey focused on leaders' views of cyber security careers, and the potential role of Cyber Discovery in developing an interest among students in this area.

Providing advice and referrals

Club Leaders generally reported feeling comfortable providing advice to young people on digital or cyber security careers (22% agreeing strongly and 36% agreeing) but were less likely to agree that the right resources were available either in-school (13%, 23% respectively) or outside school (7%, 20%).

This suggests a potential role for any programme in supporting Club Leaders through either providing relevant resources or ensuring that they can signpost students to relevant information. In interviews, Club Leaders suggested that more interactive materials, such as videos showcasing the skills required to enter relevant cyber roles, would be useful to embed in lesson plans and show at careers events and open evenings. It was also noted that interaction with external stakeholders, such as employers or universities tend to be more impactful than sessions delivered by teaching staff.

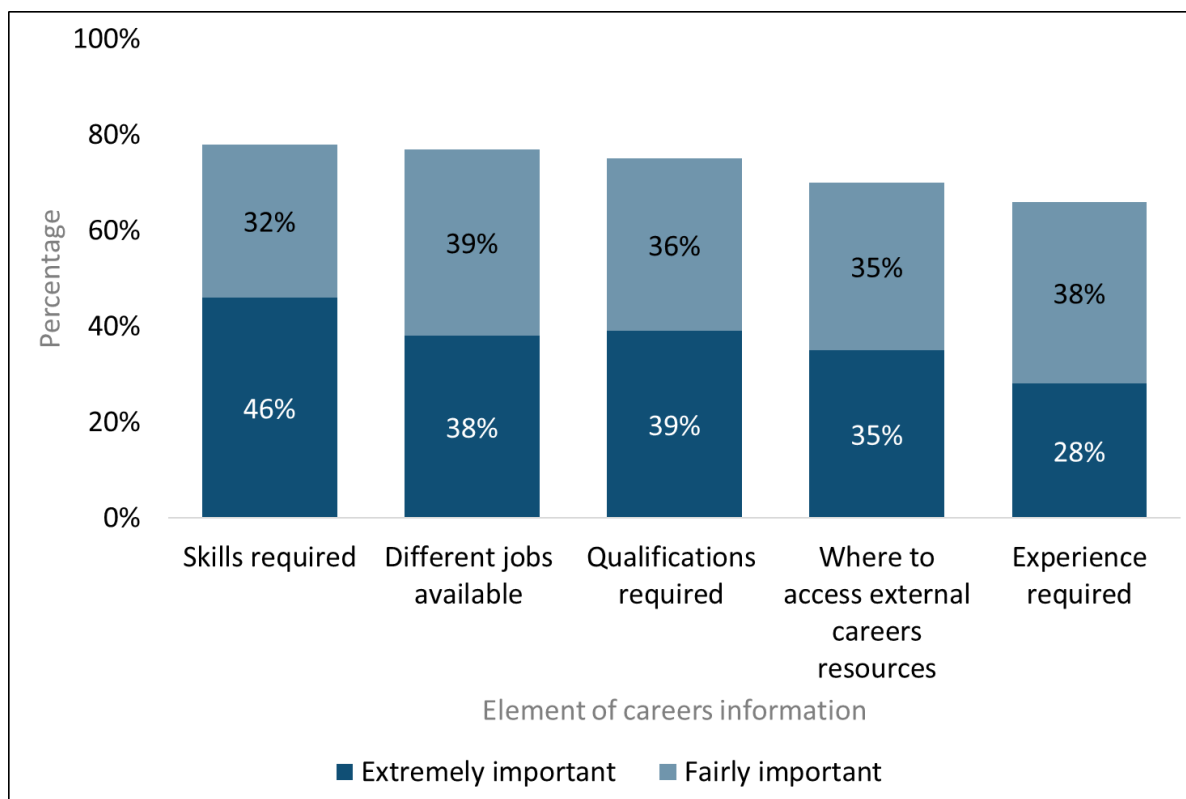
Online platforms and careers

All Club Leaders taking part in the Club Leader survey were asked how important they felt it was (using a five-point scale) that any online cyber security learning platform provided real-world examples and interaction.

Almost all Club Leaders felt it was important that an online platform provided challenges or exercises that mimicked real world situations (72% score of 5, 20% of 4) or real-world examples of the importance of cyber security (68%, 24% respectively). A smaller proportion (33%, 29%) felt that it should provide interactions with cyber security

employers. Figure 11 shows results for statements relating to the importance of online platforms providing a range of different types of information.

Figure 11: Importance of careers information on online platform (Year Three)



Source: Club Leader survey, Year Three. Q2. Base: 69.

Results showed leaders generally felt it was very important that an online platform provided a broad range of careers related information. Around three-quarters felt it was important for a platform to provide information on the required skills (46% at 5, 32% at 4), different jobs available (38%, 39% respectively), the required qualifications (39%, 36%) and where to access external careers resources (35%, 35%). About two-thirds (28%, 38%) felt it should provide information on the experience that would be required.

Range of participants

Identifying most talented

As set out in the Theory of Change, one of the programme's outcomes is to identify the most talented participants. MI data shows that over the first three years, the number of participants identified as 'Elite' increased from 287 in Year One to 487 in Year Two, 624

in Year Three, and 778 in Year Four.²⁷ Elite students' were defined as students scoring 13 or 14 on CyberStart Assess (out of a maximum possible score of 14), having broken into HQ level 10 and 11 (completing at least one challenge in both) and having "demonstrated keen interest in the cyber security industry" by attending at least one additional careers event, such as a webcast, industry event or careers fair.

A number of these Elite participants went on to attend Elite Camps: 170 in Year One, 180 in Year Two, and 240 in Year Three. Therefore, in addition to engaging a large number of participants, Cyber Discovery also identified over 1,300 Elite students and delivered additional training and support to 590 of those through Elite Camps. The Elite Talent Development Programme, introduced in Year Three, also provided additional training to 32 of the top performing Elite participants across all three years, with the specific aim of encouraging them to pursue careers in cyber security over other options.

As noted previously, industry experts generally felt that Cyber Discovery helped identify talented young people, making sure that those progressing to later stages had the required technical and soft skills. This includes those achieving GIAC qualifications who represented a small number in absolute terms (especially compared to the skills gap) but the largest number of teenagers ever achieving this certification. As these provided an industry standard qualification they allowed experts to easily assess the performance of students sitting this exam.

Club Leaders and students also felt that the programme broadly helped identify the most talented although, as noted previously, some felt that the most talented may find the Assess level too basic. Elite Camps were key, with most of the industry experts involved feeling these successfully identified talented participants although some questioned whether the amount of academic or extra-curricular demands may stop some from progressing.

Diversity of students

Several Club Leaders and students felt the greater proportion of male than female participants in their Cyber Discovery clubs was generally reflective of the gender balance in computer science classes. As outlined previously, MI shows that Cyber Discovery has a higher proportion of females aged 14 to 16 participating (28%) than GCSE Computer Science (22%). There were also higher proportions of ethnic minority participants in Cyber Discovery (29%) compared to the proportion of 2017 ethnic minority GCSE (22%) and A-level (25%) participants.²⁸ However, engaged schools were disproportionately focused in the South of England, suggesting that regional diversity could be improved.

²⁷ Since some participants participated in Cyber Discovery across more than one year, it is possible that the same participant may have been identified as Elite in more than one year.

²⁸ [The Roehampton Annual Computing Education Report: Data from 2017](#)

Feedback from Club Leaders suggested that Cyber Discovery suited students who could focus on tasks and had the determination to find solutions through independent learning. One Club Leader noted that their autistic students tended to be particularly successful as they were driven to solve challenges and reach a conclusion.

Several suggestions were made to increase the diversity of students taking part in the programme, often including approaches that had already been implemented by Cyber Discovery to various extents. Suggestions included ensuring marketing materials feature gender and ethnicity balanced images; developing mentoring initiatives for students taking cyber security as a career or further academic study; targeting schools in areas of deprivation; ensuring all students have access to a suitable computer and internet connection; and financial support for schools to set up clubs where students can access a network that is separate to the school network.

Additional Club Leader outcomes

A theme among some Club Leaders was that being involved in Cyber Discovery had helped them develop cyber security knowledge and skills, with these contributing to delivering more or better information in school:

“It’s kept my narrow focus of subject knowledge up to date and provided context so when students ask about that area, I’ve got a bit more to say.” Club Leader

Some leaders felt that being a leader helped them build on good levels of prior knowledge. One Club Leader taught the National Progression Award (NPA) in Cyber Security and noted that their involvement in CyberFirst and Cyber Discovery had given them a better understanding of the language used on the course. Several said they would value the opportunity to undertake further training and share ideas with other leaders, for example through an online forum or club.

Club Leaders also identified outcomes for the wider school, for example by showcasing to parents that their students are able to access competitions and have the opportunity to progress.

“Parents are always keen to find out about extra-curricular activities that do not cost anything, but will help stretch their children.” Club Leader

One Club Leader said that where they had particular success with some of their students taking part, they were able to cite that in applications to become a national computing centre.

“There is kudos attached if you have success. We’ve also featured students in press releases where they’ve gone quite a way. It’s positive publicity.” Club Leader

As mentioned above in the ‘reasons for taking part’ section, Club Leaders in CyberFirst accredited schools are able to use Cyber Discovery to help achieve their wider aim to encourage students to engage with computer science and the application of cyber security in everyday technology.

Programme impact and the skills gap

This section assesses the potential contribution of Cyber Discovery to closing the cyber skills gap. This is a long-term programme aim and there are many factors that may help close the gap. Measuring the precise impact of Cyber Discovery on the skills gap is beyond the scope of the evaluation as this would likely include the development of a counterfactual approach to assess whether any participant outcomes would have occurred regardless. As a result, brief information is included to cover initial perceptions around whether the programme may be closing the gap and suggestions from qualitative interviews as to how this could be maximised.

Perceptions of the skills gap and existing mechanisms

As noted in the Introduction, it is estimated that 48% of businesses in the UK have a basic technical skills gap in areas including setting up configured firewalls, storing or transferring personal data, and detecting and removing malware. Research has also shown that there are misconceptions about the skills required to fulfil a cyber security role and highlighted the need for candidates with a broad set of technical expertise and skills, complemented by the right soft skills to do the job effectively.

Students generally felt that the programme would help to close the gap, albeit that this largely reflected their own positive experiences of the programme. Most felt that they would probably have had an interest in cyber security, but without taking part they would not have had the same level of insight into the sector. This helped some to refine their future career plans with, as seen earlier, data showing that the proportion of respondents very interested in a cyber security career did not increase from pre to post stages.

In Years Two and Three of the evaluation, industry experts shared their views on the skills gap and suggestions for further action. As discussed, experts highlighted a range of benefits which they felt was evidence of the potential of the programme to contribute to closing the skills gap. For example, some had recruited placement students and apprentices and noted that participants, particularly those reaching Elite stage, tended to be high calibre candidates.

Cyber Discovery was felt by some experts to address the key area of the skills pipeline by encouraging a diverse range of students to pursue a cyber security career who otherwise may have entered technical roles in other sectors. As many students are still in education, it was recognised that it may be years before the impact is realised. However, experts were confident that Cyber Discovery was raising awareness of roles in the sector and equipping students with the knowledge and skills needed.

“Cyber Discovery has broadened my knowledge of the roles that the umbrella term of cyber-security covers, and it's not all hacking. There's the forensics and reverse engineering malware side, which I have almost fallen in love with. And this was all due to Cyber Discovery, which led me to google and expand my horizons.” *Year Four student*

One student noted that it was particularly beneficial to take part in a government led programme rather than one that was industry sponsored. They saw a greater role for an organisation such as the National Cyber Security Centre (NCSC) in communicating the pathways into the sector.

“SANS will channel you to GIAC, OffSec will channel you somewhere else. It would be nice if the NCSC played a greater role in communicating with young people.” *Year Four student*

Additional mechanisms to close the skills gap

A range of views were presented on the priority areas to reduce the skills gap, with common themes being a lack of specialist knowledge and the lack of alignment between the demands of industry and what potential candidates are taught in formal education. Some felt that graduates often had a clear grasp of theoretical issues but struggled to apply their knowledge to a business setting. In their view, educational establishments should be supported to give better industry specific careers guidance to students, for example how to answer behavioural questions and complete psychometric tests.

Regional differences were highlighted, for example the problem of ‘brain drain’ where graduates in certain areas leave because they do not think high value industry and progression are available to them there.

Another felt there was a gap in certain specialisms. In their experience, candidates tended to have a general technology focus rather than having a specialism and were often not aware of the range of roles available to them, especially with ethnic minority groups and female candidates. They suggested that any initiative should be representative of the whole sector and feature a diverse range of roles, for example less emphasis on pen testers. It was suggested initiatives do more to recognise the breadth of the portfolio, for example making sure that training is aligned to the wider elements of cyber security, including compliance, governance, risk and strategy.

A further theme was the need to improve public knowledge of cyber security. It was noted that parents, teachers and friends were all likely to influence students’ decisions about careers, therefore requiring wider acceptance of cyber security as a viable careers

option. This is supported by survey data, which showed that for around a quarter of respondents, their decision to participate in Cyber Discovery was influenced by a teacher or friends. Another industry expert identified a gap in further and higher education:

“When you get to sixth form or college, it’s all gone.” *Industry expert*

They suggested that there is a need for a continuous pathway to ensure that when young people are focused on apprenticeship or job applications, they retain their focus and interest in cyber security. They proposed an expansion of the University Technical College (UTC) model, with business sponsored projects based around industry problems. This links to qualitative feedback from curriculum experts and Club Leaders who would like to see formal cyber security qualifications introduced, for example a GCSE or T-Level. As noted in the ‘links to the curriculum’ section, it was suggested that this could provide an alternative to the “programming-heavy” computer science courses, which can put off female students.

“We’re definitely crying out for a vocational GCSE as an alternative to computer science. There’s a real market for a GCSE in cyber security, especially for girls. They love that problem solving element, the idea of doing good in the world is really motivating. Programming less so.” *Curriculum expert*

Students suggested that programmes could give them more information about the specific requirements for entry level roles in the sector and where to find jobs.

“The whole industry doesn’t seem very accessible. There aren’t too many jobs around and it’s not clear what you need for each job. There are no subjects in school for it. There certainly isn’t a shortage of people who want to get into it, but some decide they want to be a software developer instead because it’s more clear what you need to learn.” *Year Four student*

Conclusions and recommendations

This section provides a short conclusion drawing together the main strands of evidence followed by a core set of recommendations.

Conclusions

The programme met the key performance indicator in the original contract. This was to engage almost 6,000 participants by the end of the fourth year, with the overall number of those registering increasing from 27,903 in Year Two to 35,941 in Year Three, dropping to 28,232 in Year Four²⁹.

In the final two years, the programme exceeded the soft target of 30% females introduced at Year Three. This was achieved in part through opening up the programme to 13-year-olds and targeting females in this age range. Participation appeared highest in areas with lower levels of deprivation and, in England, outside the South. The large difference in engagement across regions suggests the potential for wider geographic growth, but also highlights difficulties in achieving regional diversity. The proportion of ethnic minority participants was higher for Cyber Discovery than for computer science GCSE or A Level equivalents.

Participants generally progressed positively through the programme. Some struggled in the initial stages, potentially as despite a relatively gradual introduction there may always be some students that are not suited to the programme at that time. The programme provided additional training to 590 most talented participants through Elite Camps, and there was a high pass rate among those who went on to sit GIAC exams. Participants felt there was enough support in place, and one theme from Club Leader interviews was feeling that they could be helped more to support students in their clubs.

Over a third of Cyber Discovery participants (38%) had taken part in other programmes recently and many were also interested in a wide range of careers and subjects. They were very interested in cyber security but were by no means solely focused on this for future subject choices or careers. They took part in the programme largely to improve their skills, although a large minority did see the programme as helping them with possible careers.

Participants enjoyed taking part in the programme, finding it engaging, positive and useful. They felt it was challenging – although some struggled in the initial stages, they generally saw the level of challenge, often going far beyond the cyber security content of the Computer Science GCSE, as a strength of the programme. They felt tested and

²⁹ A discussion about the possible reasons for a decline in the number of registrations in Year Four is presented in the 'Total participation' section above, centred around the impact of school closures.

enjoyed proving their ability. Evidence suggests that this linked to the main strength of the programme in directly improving cyber security skills.

Survey data shows self-reported participant improvements in relevant cyber security skills, and their understanding and knowledge of job requirements but there is no evidence that this translates into increased interest in studying cyber or taking up a relevant career.

The lack of evidence of increased interest may be due to the small sample size, that providing relevant information made some realise it was not a relevant career for them earlier than they might have, or that external factors unconnected with the programme had a negative effect. It may also be the case that for many students, interest in cyber security careers was already high before participating in Cyber Discovery, so interest levels remained similar rather than increasing. Interviews suggested that for some students, the programme confirmed their interest in the subject rather than introducing a new idea. Those attending Elite Camp felt they benefited from the careers advice provided during this phase, with there being less evidence that those who did not reach this stage directly picked up career information. The relative lack of cyber career information in the early programme stages may also explain the lack of evidence of positive change in cyber career interest. Furthermore, lack of evidence around change in cyber career interest may reflect the fact that the initial objective of Cyber Discovery was to identify and support an elite cohort of already engaged and talented individuals, rather than to target a wider audience.

Industry experts were very positive about their involvement, again feeling that the Elite phase was particularly beneficial. They felt that Cyber Discovery helped develop the skills of the most talented attending the Camp and were positive about the range of different students attending.

Recommendations

While the main body of the report provides many specific recommendations, the following broad underpinning areas are included below. The first set of recommendations relate to the programme itself while the second set of recommendations relate to the positioning of Cyber Discovery in the wider marketplace, largely drawing on suggestions from curriculum experts and industry experts about what more could be done to address the cyber security skills gap.

Programme Recommendations

Programme Recommendation 1: Continue to increase diversity

Increasing the diversity of those taking part in Cyber Discovery is important not only in its own right but also for ethical reasons and as a potential means to reduce the skills gap. This reflects well-known challenges in the sector and across STEM subjects as a whole in this area. This is also important given that around a third of participants did not agree strongly or agree that cyber security careers were open to everyone regardless of background.

Data in this report suggests that opening the programme to those aged 13 has made a considerable contribution to increasing gender diversity across the programme, in part likely due to targeted marketing to girls in this age group. This cohort should be tracked in detail to begin to assess whether their participation at this stage facilitates engagement beyond what was achieved in previous years where the programme was only open to those aged 14 and over.

Further programme and sectoral learning can build on information in this report on successful approaches for engaging female students. It is important that these key strengths are built upon, for example facilitating communities of female students. Similar approaches should be examined for socio-economic diversity, examining issues identified in this report on access to suitable technology, raising awareness of bursaries and apprenticeship routes to remove perceived financial barriers to higher education, and the overall reach to schools in deprived areas. This may be particularly important given the relatively high level of interest in studying or having a career in cyber security among those in state schools compared to those in private or other types of school.

Programme Recommendation 2: Examine and embed career consideration

As the Theory of Change details, a key intended impact of Cyber Discovery is that it helps improve consideration and take-up of cyber security careers, thereby contributing to reducing the cyber security skills gap. Therefore, the extent to which Cyber Discovery changes career consideration is a crucial question for future programme development. Information in this report suggests it should not be automatically assumed that taking part leads to improved career consideration although it may be that increased knowledge leads to a better alignment of career options among participants, including some understanding it is less of an option for them.

Further work is required to provide a solid evidence base on this issue. This could include embedding simple questions on career consideration into any registration (at least for those aged 16 and over who can provide consent), with this facilitating longer-term follow-up and potential links to later administrative data on further and higher education choices.

Information on careers throughout the programme should be expanded to ensure that this is not just prioritised at Elite Camp stage. This should include making information as transparent as possible to Club Leaders given the lack of confidence and availability of resources affecting some.

Programme Recommendation 3: Improve support and guidance for Club Leaders and students

Improved support and guidance should be provided to Club Leaders to enable them to better engage students and assist them through the challenges. Firstly, there is a need to ensure that approaches to engagement taken by Club Leaders are best suited to their specific needs. It is appropriate for Club Leaders to take a broad approach to engaging young people, particularly as this may help both create and sustain an interest in cyber security and ensure the programme continues to avoid focusing on computer science students. The challenge is to ensure that leaders and students have expectations set at realistic levels to avoid being put off participation or careers if they do not progress as planned.

The second area is ensuring that participants and Club Leaders have adequate support and guidance available on Cyber Discovery itself. Evidence from interviews suggested that some Club Leaders struggled to provide consistent support and guidance with challenges. A range of possible approaches to supporting leaders are provided in the “support and guidance for participants” section, including video walkthroughs, more signposting resources, and an online community for them to share ideas and experiences.

Wider Recommendations

Wider Recommendation 1: Consider the role of formal qualifications

A strong theme from interviews with Club Leaders and students was that the content of Cyber Discovery goes far beyond what is covered in relevant computing courses, including GCSE and A-Level Computer Science. Rather than incorporating more curriculum content into Cyber Discovery or vice versa, some curriculum experts and Club Leaders suggested that they would like to see the introduction of formal cyber security qualifications, such as a GCSE or T-Level in Cyber Security. In their view, this could present an alternative to computer science qualifications, which some students (particularly female students) find too programming heavy and this can deter them from the subject. This has important implications for addressing diversity in cyber security.

Some students found the extra-curricular aspect of Cyber Discovery highly appealing and felt that a programme that tied closely to what they were studying in school may not be as engaging and fun. Feedback also suggested that the opportunity for independent learning and research was an important outcome.

Wider Recommendation 2: Consider non-technical cyber security roles

Students generally felt that Cyber Discovery provided them with an improved understanding of the cyber security sector and the diversity of roles available. However, it was suggested that careers information was targeted towards technical roles, such as ethical hacking and digital forensics. Students and industry experts proposed that future programmes could include content relating to a wider range of cyber security roles, such as governance, policy, strategy and risk.

Wider Recommendation 3: Consider the scope of the overall cyber security portfolio

This evaluation highlights the extent that those taking part in Cyber Discovery not only have participated in other computing or cyber security programmes but that around two-thirds (65%) were considering doing so in the future. Data suggests that those taking part in the evaluation have enjoyed Cyber Discovery and feel they have benefitted. Qualitative feedback suggested that some preferred Cyber Discovery to other programmes, although there were suggestions that other programmes had certain strengths as well.

Survey data suggests that Cyber Discovery may have a distinct image compared to other programmes, in particular being seen as more challenging and providing a longer time frame so students can take part in their own time around other commitments. Cyber Discovery also provides a high-level of achievement for the most talented, including very high levels of certification via the GIAC exams in the Elite phase.

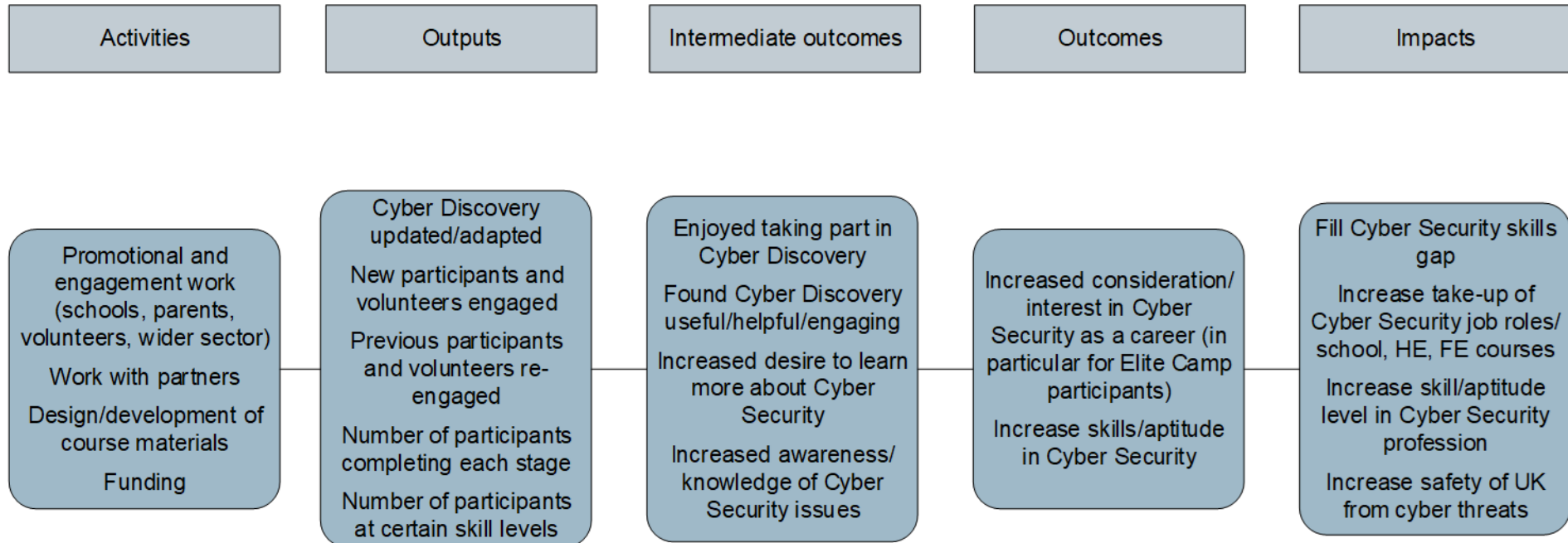
The image and offering of Cyber Discovery needs to be considered in line with the rest of the CyberFirst portfolio and other existing or potential programmes. While developing the skills of the most talented, Cyber Discovery also engages large numbers of participants, many of whom develop skills and progress through the programme but without reaching Elite Camp stage. Developing the offering into a year-round learning option would provide opportunities to engage more students on a regular basis.

This represents an ongoing challenge across the CyberFirst portfolio as a whole, in understanding the contribution of different interventions in terms of:

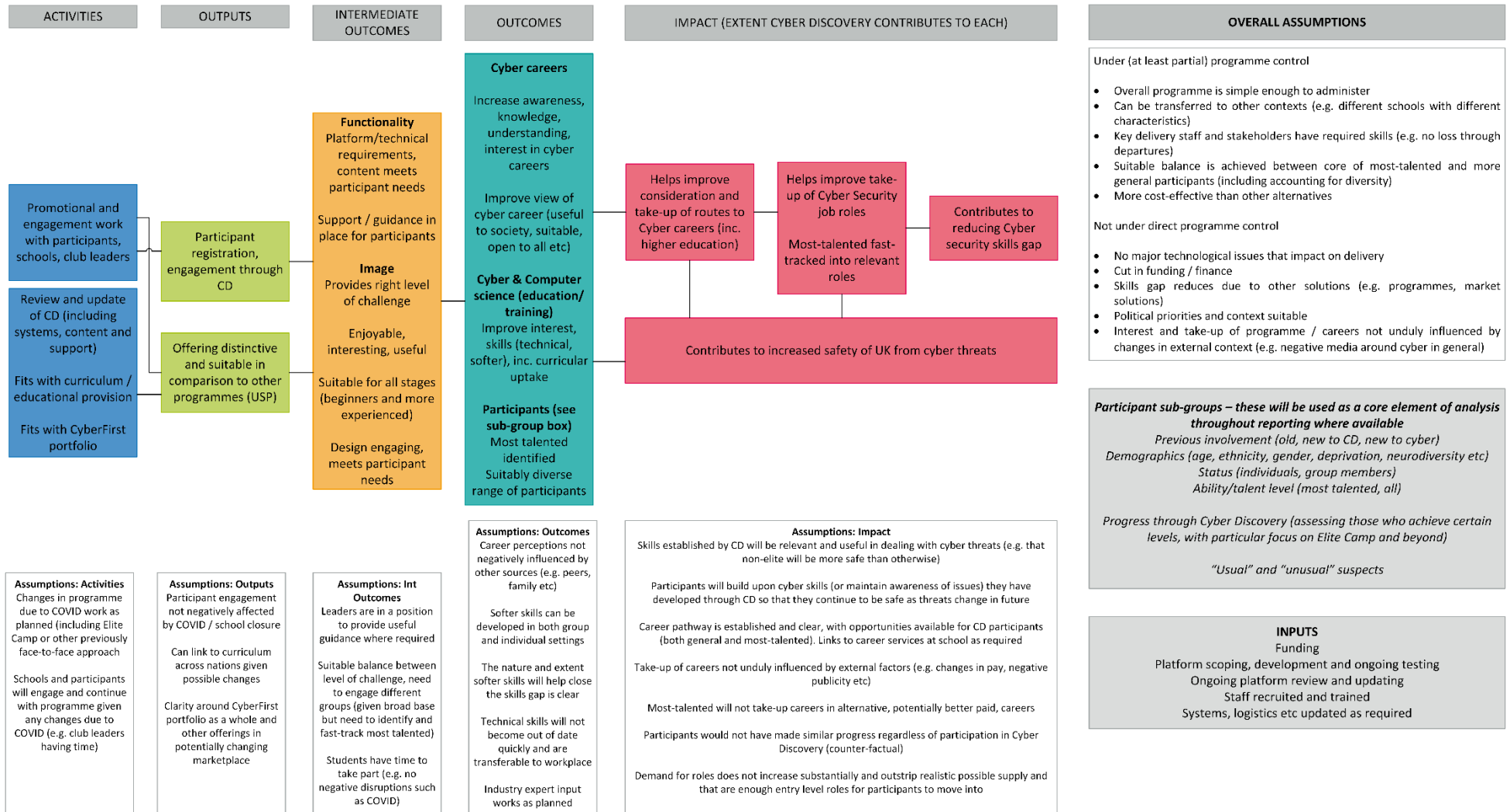
- engaging a broad base of participants, particularly in the early years when curriculum options are still open
- identifying the most talented and ensuring there is sufficient support in place to facilitate career choice, especially among older participants
- ensuring that a sensible balance is in place across any portfolio, with similar options being potentially valuable but only if this provides genuine choice, is not confusing to participants or schools, and enables cross-programme sharing of learning

Appendix One: Theories of Change

2018 Theory of Change:



2020 Theory of Change:



Appendix Two: Tables and Figures

Table 9: Demographics for participants registered for Assess by year

	Year One	Year Two	Year Three	Year Four
Gender³⁰				
Female	21%	25%	32%	33%
Male	79%	75%	68%	67%
Age³¹				
13	NA	NA	28%	27%
14	36%	36%	26%	24%
15	29%	23%	19%	18%
16	20%	17%	14%	16%
17	12%	20%	11%	11%
18	4%	3%	3%	5%
Country³²				
England	100%	93%	88%	88%
Northern Ireland	NA	1%	2%	1%
Scotland	NA	5%	7%	8%
Wales	NA	1%	3%	3%
Status³³				
Club participants	56%	51%	53%	41%

³⁰ Percentages for gender are calculated on base sizes of 17,264, 24,296, 35,887, and 28,232 for Years One to Four respectively. These bases do not include very small proportions of participants who reported another gender or did not state their gender.

³¹ Age percentages for Years One and Two are not directly comparable with Years Three and Four, where the minimum age was lowered to 13. Percentages for age are calculated on base sizes of 16,845, 24,742, 33,536, and 28,253 for Years One to Four respectively.

³² In Year One the programme was only available in England. Percentages for country are calculated on base sizes of 23,692, 34,120, and 28,232 for Years Two to Four respectively.

³³ Percentages for club and non-club participants are calculated on base sizes of 18,293, 24,251, 35,570, and 28,232 for Years One to Four respectively.

Non-club (individuals)	44%	49%	47%	59%
Whether new or returning³⁴				
New	NA	84%	82%	74%
Returning	NA	16%	18%	26%

Source: Management information.

³⁴ Percentages for new and returning are calculated on base sizes of 24,251, 35,570, and 28,253 for Years Two to Four respectively.

Table 10: Programme awareness and participation

	Ever heard of		Ever taken part in		Taken part in last 12 months ³⁵		Would like to take part in	
	Y3	Y4	Y3	Y4	Y3	Y4	Y3	Y4
Other online coding course (e.g. Khan Academy, Blockly, Tynker etc)	52%	65%	27%	39%	18%	-	35%	-
CyberFirst – Girls’ Competition (total)	32%	59%	11%	17%	5%	-	13%	-
<i>CyberFirst – Girls’ Competition (female respondents only; Y3 n=226, Y4 n=81)</i>	49%	78%	28%	39%	14%	-	31%	-
CyberFirst – summer courses	29%	56%	8%	25%	8%	-	24%	-
Other after-school or holiday coding clubs (e.g. Code Club, CoderDojo etc)	28%	65%	10%	15%	7%	-	15%	-
Cyber Centurion	22%	29%	3%	14%	3%	-	17%	-
Matrix Challenge	5%	12%	<1%	7%	<1%	-	5%	-
Any	73%	86%	48%	75%	38%	-	73%	-
<i>Base: Total sample</i>	<i>(595)</i>	<i>(196)</i>	<i>(595)</i>	<i>(196)</i>	<i>(595)</i>	-	<i>(595)</i>	-

³⁵ “Taken part in last 12 months” and “Would like to take part in” were only asked at Year Three, which is why results are not reported for Year Four.



Department for
Digital, Culture,
Media & Sport

© Department for Digital, Culture, Media and Sport 2021