Last Updated: 17/09/2025

UK Cyber Leaders Challenge Rules

Inspiring, empowering & connecting students from any background to become future cyber leaders.

Version	Date	Changes
1.2	16/09/2025	Updated competition dates & eligibility descriptors to include apprenticeships & PhD students.

1. Overview

1a. What is the UK Cyber Leaders Challenge?

The UK Cyber Leaders Challenge (CLC) is the national cyber emergency competition for UK university students. Future cyber leaders need to be equipped to handle an increasingly complex threat landscape. They need to be able to understand complex issues, manage incidents and communicate with & co-ordinate a variety of stakeholders from across government & industry in the UK and internationally.

This competition is designed to equip student competitors with technical understanding and human-centric leadership skills such as critical thinking, strategic awareness and effective collaboration to prepare them for a successful career in cyber.

We bring together government, industry & academia to support students from all backgrounds to become the UK's future cyber leaders.

The competition is split into three stages:

1. Application Process
2. Regional Qualifiers
3. National Finals

Student teams will be challenged to respond to an evolving scenario involving a national cyber emergency. They will assess issues, dependencies, risks before exploring multiple courses of action & making recommendations for the best response in terms of resilience, impact management, publicity and reputation.

A panel of judges, composed of cyber professionals, will score teams based on their analysis of the scenario, proposed responses and communication. There will be plenty of feedback from judges, ensuring that all competitors are able to enhance their skills.

Alongside the competition, students will be able to take advantage of networking and other career development activities. The direct access to established cyber professionals from a range of different backgrounds working in a range of different roles is a unique opportunity and a highlight of the competition.

1b. Key Dates

- Application Deadline: 11:59am 15th December 2025
- Release of Scenario Stage 1: 13th January 2026 (To be confirmed)
- Deadline for Regional Event Submission: 13:00 2nd February 2026 (To be confirmed)
- Regional Events: Early Feb 2026 (To be announced by November)
- National Finals: Mid-March 2026 (To be announced by November)

1c. Contact

Any queries or concerns about the rules or competition, please visit www.cyberleaderschallenge.com or contact info@cyberleaderschallenge.com.

2. Competition Format

The Cyber Leaders Challenge consists of an application process followed by four competition rounds. Teams must use their skills to consider the implications of the evolving incident and develop recommendations to respond as the scenario escalates.

2a. Application Process

Teams of four students, studying at a UK Higher Education Institution (such as a university), must submit their completed application forms by the application deadline.

The Application deadline for the 2026 UK Cyber Leaders Challenge will be 11:59AM on Monday 15th December 2025.

Student teams will then be assessed to decide which teams will compete in the Regional Qualifiers. All teams will be notified via email once a decision has been made.

Teams will be notified by 12th January 2026.

2b. Regional Qualifiers

Up to a total of 120 teams will be invited to compete in this round. There will be three hybrid Regional Qualifier events - taking place in the North-West of England, the South-West of England and Scotland. Each one-day Regional Qualifier will consist of teams competing in-person and online.

All students are expected to attend and participate fully in the activities arranged whether competing in-person or virtually.

The Regionals Qualifiers will take place in early February 2026.

Approximately, one month prior to the event, teams will receive a detailed Scenario Stage 1 setting the scene for an ongoing incident that could be of concern to regional authorities and the government.

Teams will be expected to analyse the material, conduct research and use their own skills to prepare a 10-minute Briefing, supported by a Briefing Note.

At the end of the round, teams will receive feedback from the panel of judges. Judges will score the teams based on the marking criteria provided by the Cyber Leaders Challenge team. The judges' will score teams based on a combination of their Briefing and Briefing Note.

Once all scores are collated, 17 teams will advance to compete in the National Finals.

Each deliverable is detailed below:

Briefing Note

Before their Briefing, teams are required to submit a PDF document, up to two single-sided A4 pages (one doubled-sided sheet) in length. This note will be given to judges 2-minutes before the team's Briefing.

It should support the team's ability to communicate to the judges effectively. The Briefing Note should include the team's critical analysis of the situation, the implications of the cyber incident, their recommendations for managing the impact of the incident and any other issues to be considered.

Teams must email this document to info@cyberleaderschallenge.com by 13:00 on Monday 2nd February 2025 (TBC).

Briefing

Teams are expected to explore and analyse the key issues and implications related to the cyber incident described in the Scenario Stage 1 document. This 10-minute Brief is expected to provide a concise assessment of the situation, address potential impacts & risks and discuss the implications.

It provides an opportunity to highlight the key elements of the scenario including any national security concerns, demonstrate the team's ability to critically analyse the scenario, assess the suitability of multiple options for managing the impact of the incident and address any other issues. It will cover the advantages & disadvantages of various response options and explore the course of action being recommended.

Following the Briefing, teams will receive 10 minutes of direct questions from the judging panel.

Successful teams will be notified following the Regional Qualifiers and will be invited to the National Finals.

2c. National Finals

The top 17 teams across all the Regional Qualifiers will be invited to compete in the 2-day National Finals event at the BT Tower, London. There are three elimination rounds during the event, with only the top 3 teams progressing to the Grand Final round.

All National Finalist teams are expected to be in-person with no virtual option. We plan to offer a virtual element to the National Finals to enable non-finalist teams to engage virtually.

The National Final will take place over two days in mid-March 2025.

Around one month prior to the National Final, successful teams will receive a detailed Scenario Stage 2 document which will be an escalation of the existing cyber incident. As before, teams will be expected to analyse the material, conduct research and use their own skills to prepare a Briefing supported by a Briefing Note.

At the end of each round at the National Final, teams will receive feedback from the judges. The panel of judges will score teams based on the marking criteria provided by the Cyber Leaders Challenge team.

Scores in each round are treated independently, meaning they do not carry over from previous rounds. Once all scores for a round are collated, the top teams will advance into the next round.

Quarter-Final Round

The Quarter-Final Round will be held across Day 1 of the National Finals.

Briefing Note

Before their briefing, teams are required to submit a PDF document, up to two single-sided A4 pages (one doubled-sided sheet) in length. This note will be given to judges 2-minutes before the team's Briefing.

It should support the team's ability to communicate to the judges effectively. The Briefing Note should include the team's critical analysis of the situation, the implications of the cyber incident, their recommendations for managing the impact of the incident and any other issues to be considered.

Teams must email this document to info@cyberleaderschallenge.com. Further details will be included in the Scenario Stage 2 document.

Briefing

Teams are expected to explore and analyse the key issues and implications related to the cyber incident described in the Scenario Stage 2 document. This 10-minute Brief is expected to provide a concise assessment of the situation, address potential impacts & risks and discuss the implications.

It provides an opportunity to highlight the key elements of the scenario including any national security concerns, demonstrate the team's ability to critically analyse the scenario, assess the suitability of multiple options for managing the impact of the incident and address any other issues. It will cover the advantages & disadvantages of various response options and explore the course of action being recommended.

Following the Briefing, teams will receive 10 minutes of direct questions from the judging panel.

Semi-Final Round

The Semi-Final Round will be held on the morning of Day 2 of the National Finals. At this point, the scenario will run in real time.

The 10 advancing teams will be announced at the end of Day 1. Teams will receive Scenario Stage 3 document and will have overnight to analyse the material, conduct research and use their own skills to prepare a Briefing supported by a Briefing Note.

Teams are expected to use the Briefing to update the analysis of the situation and recommended responses to manage any impact, followed by 10 minutes to answer questions from the panel of judges. 3 teams will advance to the Grand Final based on the judges' score on the Briefing & Briefing Note.

Briefing Note

Before their briefing, teams are required to submit a PDF document, up to two single-sided A4 pages (one doubled-sided sheet) in length. This note will be given to judges 2-minutes before the team's Briefing.

It should support the team's ability to communicate to the judges effectively. The Briefing Note should include the team's critical analysis of the situation, the implications of the cyber incident, their recommendations for managing the impact of the incident and any other issues to be considered.

Teams must email this document to info@cyberleaderschallenge.com. Further details will be included in the Scenario Stage 3 document.

Briefing

As before, teams are expected to explore and analyse the key issues and implications related to the cyber incident described in the Scenario Stage 3 document. This 10-minute Brief is expected to provide a concise assessment of the situation, address potential impacts & risks and discuss the implications.

It provides an opportunity to highlight the key elements of the scenario including any national security concerns, demonstrate the team's ability to critically analyse the scenario, assess the suitability of multiple options for managing the impact of the incident and address any other issues. It will cover the advantages & disadvantages of various response options and explore the course of action being recommended.

Following the Briefing, teams will receive 10 minutes of direct questions from the judging panel.

Grand Final

The Grand Final, held in the afternoon of Day 2, will replicate a national cyber emergency meeting relating to the incident - similar to a COBR meeting.

Advancing teams will be announced early afternoon on Day 2. These teams will be moved into a holding room while they wait to receive Scenario Stage 4 document. Teams will receive the Scenario Stage 4 document 15-minutes before their Briefing.

Teams are expected to quickly respond to the Scenario Stage 4 document that further develops the scenario. Teams will be tested on their ability to analyse information as a team and synthesise response options on the spot. Preparation & organisation will be key.

This round will be run in the auditorium of the BT Tower with all National Final teams in the audience. For this round, the judges will be top cyber leaders from the UK public & private sector.

The UK Cyber Leaders Challenge Champions will be decided from the Grand Final scores.

Briefing

As before, teams are expected to explore and analyse the key issues and implications related to the cyber incident described in the Scenario Stage 4 document. This 10-minute Brief is expected to provide a concise assessment of the situation, address potential impacts & risks and discuss the implications.

It provides an opportunity to highlight the key elements of the scenario including any national security concerns, demonstrate the team's ability to critically analyse the scenario, assess the suitability of multiple options for managing the impact of the incident and address any other issues. It will cover the advantages & disadvantages of various response options and explore the course of action being recommended.

Following the Briefing, teams will receive 10 minutes of direct questions from the judging panel.

3. Scoring

3a. Application Process

Each application will go through an internal downselection process based on a set marking criteria. We are interested in the team's ability to research, analyse multiple viewpoints and communicate their response to the question.

Teams will be notified by email whether or not they will be advancing to the Regional Qualifiers. We encourage students of all ability levels with an interest in cyber or strategy to apply to this competition.

3b. Timekeeping

The designated Timekeeper or Lead Judge in each round will keep track of time limits for the Briefing. They will make the team aware when they have five-minutes remaining, one-minute remaining and when time is up. At this point, the team must finish their Briefing.

3c. The Scenario

All competition rounds are based on a single escalating national cyber incident scenario. The scenario is presented to teams through four Scenario Stages. Scenario Stage documents will be distributed via email to ensure all teams have equal opportunity to analyse the material & prepare their response.

The scenario is fictitious and designed for the Cyber Leaders Challenge only.

3d. Judging

Each round of the competition will be judged by a panel of cyber professionals using a marking criteria provided by the Cyber Leaders Challenge. Judges will change between sessions subject to their availability.

All teams will be evaluated based on four main pillars of their responses: understanding of cyber issues; appreciation of the incident within broader context & wider issues; quality & presentation of proposed responses; and teamwork & communication.

The scores from this marking criteria will be used to determine the team position at each stage of the scenario. Score do not carry over to subsequent rounds unless a tie break is required.

At the end of the Regional Qualifiers, we will announce which teams will be advancing to the National Final. In the event of a tie, we will use the Application scores of each team to decide. We reserve the right to determine additional tiebreakers should they be required.

At the end of the Quarter-Final Round during the National Final, we will announce which teams will be advancing to the Semi-Final Round. In the event of a tie, the team with the higher Regional Qualifier score will advance. If the teams are still tied, we will use the Application scores. We reserve the right to determine additional tiebreakers should they be required.

At the end of the Semi-Final Round of the National Final, we will announce which teams will be advancing to the Grand Final. In the event of a tie, the team with the highest score from the Quarter-Final Round will advance. If the teams are still tied, we will use the Quarter-Final Round tiebreak method. We reserve the right to determine additional tiebreakers should they be required.

At the end of the Grand Final, we will announce the UK Cyber Leaders Challenge Champions based on the consensus of the VIP judges for this round. If a decision cannot be made, we reserve the right to determine additional tiebreakers should they be required.

4. Celebrating Success

4a. Team Progression

During the competition, all teams are expected to participate in the range of activities being provided alongside the competition rounds and spectate the Grand Final Round of the competition. This includes the networking opportunities, keynotes and other sessions running alongside the competition.

We will aim to provide career development opportunities to all teams that apply for the Cyber Leaders Challenge.

Eliminated teams may still win team awards for their performance in the competition.

4b. Awards

In addition to the main competition, we will award additional prizes for outstanding achievement. The categories of prizes to be offered will be announced at the start of the competition.

4c. Media & Publicity

Invited external spectators may be present at both the Regional Qualifiers and the National Final. We will brief the spectators to limit the impact they have in disturbing or assisting any of the competing teams.

The Cyber Leaders Challenge reserves the right to use media (photography, videography & audio) from the event to support and promote competition aims. Whilst respecting individuals privacy, it is anticipated that participants will be willing to be photographed participating in any of the organised activities during the competition, including but not limited to competition rounds, workshops, networking sessions and careers fairs.

The Cyber Leaders Challenge organising team remain cognisant of personal concerns relating to the use of their image. Exceptions to this can be discussed with the Competition Director. All attendees at any Cyber Leaders Challenge event must conduct themselves in a respectful & professional manner.

5. Eligibility

5a. Coaches

Each team should recruit a coach to support them during the competition. The coach is not an active competitor in the competition but plays an important role in supporting the team's learning & skill development.

Coaches:

- can be anyone but most coaches will be university lecturers. Coaches do not need to be affiliated to the same Higher Education Institution or employer as the team members.
- can coach multiple teams.
- should, but are not required to, have cyber, national security or politics knowledge or experience to be able to best support their team.
- should support their team by asking questions, helping students to learn independently & providing feedback, rather than prescribing a specific method to approach the competition & scenario.
- are encouraged, but not required, to attend their team's Regional Qualifiers and the National Finals, should the teams progress in the competition.

    - Coaches may observe their team's Briefing Round and make notes but may not actively contribute.
- There is no prescribed time commitment for coaches. However, as a minimum we would advise that coaches are prepared to spend 3 hours supporting their team before the Regional Qualifiers.

If a coach is not affiliated with any team members' UK Higher Education Institution (HEI) or employer, the team must a HEI or employer Point of Contact for safeguarding purposes.

If your team is struggling to find a coach, please email info@cyberleaderschallenge.com before applying to request support.

5b. Student Competitors

We strongly encourage you to read the eligibility before forming your team and get in touch early if you have any questions.

All teams should meet the following criteria to be eligible for the competition:

- Teams should consist of four members. Teams of three will be considered at the discretion of the Competition Director.
- Each team member should be 18 years of age or older at the time of the Regional Qualifiers in February 2026.
- Each team member must be currently studying on a Level 4 or above (Level 7 or above in Scotland) course or apprenticeship at a UK organisation. This includes students on Foundation, Undergraduate, Year in Industry, Postgraduate, Apprenticeship, Study Abroad, Exchange, PhD or other programmes.
- Each team member must not have substantial professional experience in any industry that gives them a significant advantage in the competition (details below*).
- Each team member must not have substantial professional experience in responding to a cyber incident or briefing C-Suite / senior management (details below*).

*What we mean by professional experience.

The spirit of the competition is to support students who are at the beginning of their cyber career and who do not have significant professional cyber experience.

We do not consider Internships, Apprenticeships or Year in Industry placements to be significant experience, unless a core part of your role involved responding to cyber crises or briefing senior management.

Here are a few example personas, who are all studying on a Level 4 or above programme in the UK but have prior professional experience which may affect their eligibility.

Eligible	Get in Touch	Not Eligible
4-years working part-time in a retail store or supermarket	Director of a not-for-profit initiative or small business	4-years in a role briefing senior management
Completed an 8-week internship as a policy analyst	1-year full-time employment as a policy analyst	2-years full time employment as a policy analyst
5 years full-time employment as a software developer	1-year full-time employment in a policy role outside the UK	
Completed a year-in-industry in threat intelligence	Experience through compulsory military service	
	2-years experience working with Think Tanks or public bodies	

Everyone's level of experience is unique, so it's important that you are proactive in checking your eligibility with us if you are unsure.

If any of the following statements apply to you, please email info@cyberleaderschallenge.com outlining the details of your experience why you believe it does not give you an unfair advantage in the competition **before submitting your application**.

- You are unsure about your eligibility to compete.
- You have limited experience in responding to cyber crises or briefing senior management.
- You have over 1 year of professional experience in any industry.

If your eligibility is queried by our organising team after you have submitted your application, it may lead to your team not being allocated to your preferred Regional Qualifier or team disqualification.

You should also be aware that:

- Multidisciplinary teams are encouraged but not required.
    - For example, a team comprising of a mix of politics, law, economics and computer science students may have an advantage over a team of only computer scientists.
- Team members can be in any year of study.
    - In 2025, several first-year teams made it to the National Finals - outperforming teams in later years of their degree.
- Teams can be comprised of team members from multiple organisations.
    - In 2025, we had a team of University of Exeter & University of Edinburgh students. The Third-Place team had students from the University of Birmingham & Aston University.
- An organisation, such as a university or apprenticeship employer, can be represented by multiple teams and there is no limit.

- For example, there could be three separate teams with team members studying at the University of Manchester.

5c. Eligibility Verification

The UK Cyber Leaders Challenge team will review each individuals eligibility on a rolling basis as students complete their profile on the application platform.

We will use your CV, LinkedIn and other sources of information to verify your eligibility for the competition.

If we have any queries or believe that you are ineligible to compete, we will contact you using the email address you provided when signing up to the application platform.

5d. Rule Breaking

Teams are encouraged to seek support to broaden their viewpoint whilst preparing their Briefings and Briefing Notes. Teams should seek guidance from their coach in particular.

All submissions must be the team's own work. Using work that has been generated wholly or in part by an AI tool, such as ChatGPT, or another person will result in disqualification from the competition. However, AI tools such as ChatGPT may be used for research purposes only. We reserve the right for final judgement on perceived AI generated content.

During Briefings, no external support is allowed. This includes the team's coach, who may only spectate their team's Briefing. Teams must only provide judges with their Briefing Note to aid their Briefing. Teams may use written or printed notes for personal use during their Briefing. If any student needs to use an electronic device for an accessibility requirement, please contact the Cyber Leaders Challenge team prior to the competition.

Rule breaking during the competition is taken very seriously. At the discretion of the Cyber Leaders Challenge Director & organising team, participants may be disqualified. All teams are expected to compete in the spirit of the competition.

The decision of the Cyber Leaders Challenge organising team is final.

6. Accessibility

The Cyber Leaders Challenge is committed to ensure that all teams compete on a level playing field. We aim to be proactive in our support of any accessibility requirements that will enable students to perform at their best during the competition.

Please contact us if you need any support at info@cyberleaderschallege.com.

7. Rule Changes

The Cyber Leaders Challenge reserves the right to alter the rules at any time. Any updates to the competition rules will result in a new version of this document being published & distributed to teams via email.