

# Invitation to Express Interest

---

**Adult EdTech Project:** Cyber Security and Hacking Lab

**Funding:** £100k

**Closing date:** 15<sup>th</sup> July 2020

## Purpose

The requirement for digital skills across all sectors of industry continues to grow apace and is predicted to be in greater demand as we emerge from the pandemic and into economic recovery. Significantly increasing the number of young people who gain digital skills is imperative for their future CVs.

WMCA is seeking to create a Hacking Lab in the West Midlands to inspire young people and raise awareness of the range of careers in cyber security. The Hacking Lab would be an ethical hacking, computer network and security challenge centre, dedicated to educating and finding cyber security talent.

It would be free to use for all schools and colleges in the West Midlands Combined Authority area supporting them to develop both their curriculum and also their clubs and wider enrichment for students.

## Project Aims

The project is designed to increase the number of young people experiencing and developing cyber skills through a fun, interactive and safe experience. It aims to support colleges, schools, training providers and teachers by making an easily accessible and free resource. Competitions will be held between different organisations to promote cybersecurity awareness.

Mission style challenges will be set to make learning about cyber security fun and interactive, where one team is given the task to protect and the other to get through those defences. This will not only raise the profile of the cyber security profession but will identify talent and provide a pipeline of people who may go onto further training and thus find employment. The Hacking Lab would also raise awareness of the risks and ethics involved in cyber security to the wider community.

The hacking lab will be to provide the following to the students in the West Midlands:

- the basics of cyber offense and defence
- hands on practice on the most popular hacking techniques
- how to apply knowledge of hacking methods to cyber security
- an insider perspective on cyber security
- the most common cyber attacks

- hacking tools and techniques
- the importance of cyber security

### Minimum Requirements

The Hacking Lab will be expected to support a broad network of schools, colleges and training providers to use technology to educate on cyber security. This should be delivered through a mix of activities, including the provision of advice, guidance, training and competitions. Organisations applying for the Hacking Lab will need to:

- show evidence of impact of their own use of technology to support teaching, including the effective use of new technology
- partnership or collaboration with a tech company
- demonstrate their capacity and capability to support other schools, colleges to use technology more effectively to help address challenges
- provide an overview of their proposed offer and how the funding would be used to support this.

All programme support will now be provided remotely during the coronavirus (COVID-19) outbreak. Once the period of disruption from coronavirus (COVID-19) has passed, the demonstrators will help organisation with their longer-term digital capability.

WMCA will oversee the projects from a strategic co-ordination point of view and to ensure that colleges and providers are supported to deliver to students. A third-party evaluator will be appointed to evaluate the impact and the value for money of the projects.

### Evaluation Process

The WMCA evaluation partner, Winning Moves, will provide both formative and summative evaluation of the project to the WMCA.

### Funding

We will fund the development of the Hacking Lab with a grant of £100,000.

Funding can be used for:

- Lab refurbishment
- Equipment including PCs, network switches
- Software
- Marketing and promotion

Payment will be awarded to the organisation, which will be accountable for compliance with the grant agreement. A review of activity and funding will be carried out quarterly by the WMCA. This review will assess progress against activity plans and will identify any risks and issues.

Funding will be paid based on a payment schedule agreed at award stage and in line with the grant agreements

### Funding Criteria

- To apply, your institution must be an education provider, charity or community organisation
- WMCA will not score applications which do not meet the eligibility criteria. There is no right

of appeal for rejected applications

## Next Steps

Proposal to be submitted no more than 15 pages to [digitalfund@wmca.org.uk](mailto:digitalfund@wmca.org.uk) including the following information:

Overview	Maximum Number of pages (A4 size)	Weighting
<b>Organisation details</b>	Up to 1 page	0%
<b>Funding</b> <ul style="list-style-type: none"> <li>• Funding requested</li> <li>• Summary of proposed costings</li> <li>• Payment schedule requested</li> </ul>	Up to 2 pages	0%
<b>Outline for demonstrator site</b> <ul style="list-style-type: none"> <li>• Aim and summary</li> <li>• Objective of site</li> <li>• Strategic implementation of technology</li> <li>• How the site will assist and improve cyber awareness</li> <li>• How the site will support curriculum delivery of cyber security</li> <li>• Operating model of site</li> <li>• Improved accessibility and inclusion</li> </ul>	Up to 5 pages	40%
<b>Tech Organisation</b> <ul style="list-style-type: none"> <li>• Organisation details</li> <li>• Partnership and collaboration details</li> <li>• Sponsorship</li> </ul>	Up to 3 pages	30%
<b>Outcomes and Impact</b> <ul style="list-style-type: none"> <li>• The need / demand / expected outcomes</li> <li>• Benefits for education</li> <li>• Benefits for students</li> <li>• How the site will support other community learning organisations</li> </ul>	Up to 4 pages	30%

## Deadline

The deadline for submission is **15/07/2020 at 12.00pm.**

Late applications will not be accepted.

Applications will be assessed by a multi organisational panel.

Providers will be advised on 30/07/2020 whether or not they have been successful.

Successful providers will be expected to start work on the project in September 2020