NOT-EQUAL

EPSRC NetworkPlus: Social Justice through the Digital Economy

Project Review Form - Mid-Term Review Pilot Project

Please submit this form before the deadline of **5pm on the 13th December to notequal@ncl.ac.uk.**

GENERAL INFORMATION	
Lead Applicant (PI): Dr. James Nicholson	**Co-Investigators (names and organisations):**
Email address: james.nicholson@northumbria.ac.uk	**Supporting Partner(s):**
Job Title: Lecturer	University of the Third Age (U3A)
Department: Computer and Information Sciences	The Old Low Light Heritage Centre
Organisation: Northumbria University	**Project Title:** Creating and Understanding CyberGuardians in Communities
	Project Reference Number: NE52

1. SUMMARY

Please provide a summary of the activities and/or initial findings of your research project to date. This also includes events, engagement activities with non-academic partners and any other activities. Please include any images or website links that could be used for dissemination purposes (at least 500 words).

The CyberGuardians project is on schedule and running as expected. The fourteen CyberGuardians who were predominantly recruited from our partners, the University of the Third Age (U3A) and the Old Low Light which is a North Shields based charity, have completed their formal training through interactive workshops with presentations, live demonstrations (e.g. password cracking) and hands on activities (e.g. phishing test). The topics covered in the training had been identified by the group themselves as well as through existing literature on older users.

The topics were covered in three workshops, each lasting three hours and were held on the university premises. A representative from U3A and the Old Low Light also attended which seemed to provide the group with some reassurance when initially engaging with the university. This relationship does require further analysis as this person has been running classes on iPad skills for a number of years and is well-respected by the group. They have provided useful feedback on both content and materials for the CyberGuardians.

The second training session was attended by a representative from Not-Equal who took photos and video. They also interviewed some of the CyberGuardians and the Principal Investigator

The training focused on three main areas: password management, scam detection and protective software. The training material was user-friendly in terms of not being technical and relating it to concepts which they could grasp such as describing the process of encryption as "juicing an orange". This was well-received (as measured by post-session questionnaires after every event).

Feedback provided through questionnaires has been very positive about the sessions regarding them as 'informative', 'engaging' and having 'improved confidence'. The following comments were received:

- Format with time for asking questions as we went along was good;
- Demonstrations were talked about as being effective for seeing what the problem actually is and improving understanding;
- By explaining how cybersecurity is connected, the advice given makes sense.

Handouts were provided at each session with enough space for the CyberGuardians to make their own notes which is what the group had requested. A glossary of the key cybersecurity terms was also provided for each session. Video recordings of the sessions have been shared with the CyberGuardians and will be made more widely available following the conclusion of the project.

The CyberGuardians have requested digital versions of the presentations and posters/fliers for them to advertise their own cybersecurity events. As they develop these, they may request more specific teaching materials tailored to the needs of their CyberCitizens, who can be defined as anyone who requires help with online security. Two of the CyberGuardians are going to run joint sessions and have a venue booked for mid-January 2020. Others have started to put into practice what they have learnt themselves and on relatives and friends in preparation for working with CyberCitizens. Many of them have acknowledged that they have improved their own cybersecurity behaviours by changing their passwords to make them stronger and are considering adopting password managers.

Each CyberGuardian has been given a notebook with clear instructions to use as a diary, in order to keep a written record of any interactions with CyberCitizens. One CyberGuardian has requested to keep an audio record and upload it, as they are concerned that their handwriting maybe difficult to read. These diaries should provide a valuable insight into how CyberGuardians approach the dissemination process, and the types of issues that older citizens face around cybersecurity. It will also help us reflect on and evaluate our training topics and methods with a view to improving the process in the future.

Each CyberGuardian will receive a "goody bag" in early January 2020 containing a range of CyberGuardian branded items such as pens, shopping bags and mugs procured specifically for this project. These are primarily intended as a thank you to the CyberGuardians for their participation in this project but will also help form a group identity and brand. These items will also serve to promote the CyberGuardians project and gather interest for CyberCitizens.

All sessions with CyberGuardians – welcome meetings, initial focus groups, and all training sessions – have been audio recorded but they have not been analysed yet. However, one of the main concerns voiced appears to be around the use of antivirus software (whether it is necessary, whether to pay for it) and scam phone calls (how to identify them, stop them, report them). One striking observation raised from the training was just how unaware this group were of the value of personal data not just in terms of being used in fraudulent activity but also in the targeting of individuals by commercial companies.

Since the training has ended, the CyberGuardians have organically formed themselves into a support network organised on a regional basis which aims to improve self-confidence and discuss best-practice. The university has provided them with some basic teaching materials which they have subsequently modified.

Please indicate if these details can be shared in a blog post on the Not-Equal website   YES

2. WORK PLAN

Please explain any deviations from your work plan, the reasons for this and plans to address the issue (up to 250 words)

Project is on time and as planned so no deviations are in discussion at the moment.

Further Information

If you have any further questions regarding this form, please contact notequal@ncl.ac.uk or 0191 2088268.