Kent & Medway CyberSchools Network (KMCSN) Terms of Reference

12th November 2023

General

1. KMCSN is an initiative of the Institute of Cyber Security for Society (iCSS) at the University of Kent.
    a. iCSS represents the University of Kent as an Academic Centre of Excellence in Cyber Security Education (ACE-CSE) with a Gold Award status and an Academic Centre of Excellence in Cyber Security Research (ACE-CSR), recognised by the National Cyber Security Centre (NCSC, part of the GCHQ).
    b. iCSS also the University of Kent as a member of the NCSC's CyberFirst programme, the UK Government's main cyber security education and awareness raising scheme for children, currently for children from KS3 only.
2. KMCSN is supported by two key local partners: the STEM Hub managed by the Canterbury Christ Church University (CCCU), and the Kent & Medway Cyber Cluster (KMCC) Ltd.
    a. Both the STEM Hub and KMCC will provide support on dissemination, communications and recruitment of members for KMCSN, and also on co-organising events and co-developing resources.
    b. The STEM Hub will also help connect KMCSN with more local schools who choose to not participate in KMCSN.
    c. KMCC will also provide support on providing local cyber security professionals as volunteers and free consultants.
3. Another key local partner on PSHE education is to be identified.
    a. One such potential partner is the PSHE Association. We welcome recommendations on other suitable organisations with a more local focus.
4. The aim of KMCSN is to provide a platform for cyber security researchers, educators, university students and other professionals in Kent and Medway to support local schools and colleges on pre-university cyber security and online safety education and awareness raising activities.
5. KMCSN covers all children and teenagers below 18 years old ("children" hereinafter unless otherwise stated), but it has a particular focus on educating, engaging and supporting children below 13 years old to supplement existing initiatives focusing more on teenagers.
    a. The threshold of 13 is the age when children are allowed to go online independently on many online platforms.
6. Topics covered by KMCSN include both technical and socio-technical aspects of cyber security, including online safety and appropriate behaviours online, privacy, cybercrime and online fraud, mis- and disinformation (i.e., media literature). The scope will be adjusted dynamically to cover more cyber-related topics required by the national curriculum and needs identified by relevant stakeholders.
    a. In the rest of the document, we will use the term "cyber" or "cyber security" to cover all these diverse topics.
7. KMCSN has a membership-based mechanism to better prioritise its activities.
8. Given its limited resources, KMCSN will prioritise support for its members. Non-members will be supported mainly by providing free resources that can be found on its website.
    a. KMCSN's website is to be set up by iCSS.

9. KMCSN will identify relevant funders and apply for funding to support its activities. It is our hope that constant funding can be secured to support a part-time admin officer and to cover part of the costs of some cyber security professionals and university/college students on KMCSN activities (especially travel costs and costs on developing and testing resources).

10. KMCSN welcomes both organisations and individuals to provide financial support to its activities in different forms, in order to make the network more sustainable in the long term.

11. The long-term goal of KMCSN is to become an independent not-for-profit organisation or a unit of a not-for-profit organisation.
    a. Before this goal becomes a reality, KMCSN will be hosted by iCSS as part of the University of Kent's school outreach activities.

Memberships

12. KMCSN's members include two basic types: organisational members and individual members.

13. Organisational members of KMCSN are local schools and colleges meeting the following two criteria:
    a. operating fully or partly in Kent and/or Medway, and
    b. providing at least some form of pre-university education to children and young people below 18 years old.

14. KMCSN's organisational members cover schools and colleges of all types, and those with less resources and educating children with a more disadvantaged and/or diverse background are particularly encouraged to join.

15. At this moment, nurseries and children's centres are not covered by KMCSN's organisational memberships, but we will consider expanding KMCSN to cover them in the future because we consider cyber-readiness of pre-schoolers is also important.

16. Each organisational member of KMCSN shall appoint one or two members of staff as the main points of contact, who ideally should include a senior leader and/or a teacher actively engaged in cyber security and/or online safety education and/or relevant extracurricular activities.

17. If an organisational member has multiple members of staff in charge of different areas of cyber security and online safety education and extracurricular activities, more than two members of staff could be appointed as additional representatives. Such cases should be submitted to the KMCSN management team for consideration.

18. Higher education institutions (HEIs) are not normally eligible as organisational members of KMCSN unless they also offer some form of pre-university education directly. In the latter case, its pre-university education unit shall be made an organisational member, rather than the HEI itself.
    a. Instead, all HEIs can be partners of KMCSN (see Clause 34).

19. KMCSN's individual memberships are for individuals with relevant skills, knowledge and capacity to bring substantial contributions for one or more areas of KMCSN's core activities.

20. Individual members of KMCSN are not representatives of their affiliated organisations, but represent themselves as individuals who bring their contributions on a personal basis.

21. School teachers focusing on relevant teaching activities (particularly ICT and PSHE), school staff and senior school leaders managing relevant aspects of school activities, and other people focusing on relevant activities (e.g., university researchers and educators with expertise on pre-university cyber security and/or online safety education and awareness raising) are particularly welcome to join KMCSN.

22. People with a more diverse background (e.g., work experience at multiple schools, in different education stages, across multiple sectors) are particularly welcome as individual members of KMCSN.

23. People without sufficient skills and knowledge on pre-university cyber security and/or online safety education and awareness raising are not normally eligible as individual members of KMCSN, but they are encouraged to become KMCSN CyberChampions (see Clause 29).
24. Non-expert people who are not eligible as individual members of KMCSN can participate in training activities of KMCSN to become eligible as individual members.
25. KMCSN memberships are free for those eligible.
    a. A paid membership model may be adopted in the future to make the KMCSN more self-sustainable.
    b. Even if a paid membership model is introduced, KMCSN will make the more essential resources and services free for all to ensure disadvantaged schools and pupils still benefit.
    c. As a general principle, paid elements of KMCSN will be more focused on bespoke solutions and services to specific organisations and individuals.
    d. KMCSN members are encouraged to contribute to KMCSN's activities by providing cash donations and in-kind support, and bring sponsors and funders to KMCSN.
26. KMCSN members are encouraged to form Special Interest Groups (SIGs) to work on specific topics and areas relevant for pre-university cyber security education for children. Some example SIGs are as follows:
    a. Based on different educational stages: primary education, secondary education, A-level, BTEC, further education, etc.
    b. Based on types of schools: state schools, independent schools, state selective schools, and special schools, etc.
    c. Based on relevant topics: online safety, privacy, authentication (passwords, biometrics and other methods), mobile phone security, cloud security, cybercrime, digital investigation, media literature and misinformation, data protection and cyber law, cyber conflict and diplomacy, etc.
    d. Based on types of activities/resources: CyberFirst, Safer Internet Days, activities for girls, animated videos, video games, children's books and readings, parental guides, teacher training materials, etc.

Activities

27. In order to maximise its outreach to more beneficiaries and to make use of its limited resources more effectively, KMCSN will focus more on creating free resources (e.g., teaching materials, guidelines, tools, evaluation methods) especially digital ones for all relevant stakeholders. Some examples of such resources as given below:
    a. Resources are for training the trainers, i.e., for those who will deliver cyber security and online safety education and awareness raising activities for children and to train other people to do the same.
    b. Resources for supporting children and their families to learn about cyber security themselves outside of school environments, e.g., group games in a home setting.
    c. Resources for facilitating data collection and evidence building from various cyber security and online safety education, self-learning and awareness raising activities, in order to support more rigorous and scientific research and innovation on pre-university cyber security education.
28. In addition to producing resources, KMCSN will provide free consultancy services to its members and other relevant stakeholders on matters related to pre-university cyber security education in Kent and Medway, nationally and internationally.
    a. It is generally expected that those who are served join KMCSN as members.

b. We need more cyber security professionals, teachers and university students with the right skills and interests to volunteer as such consultants.

c. It is our hope that long-term funding will be secured to support such consultancy services, in order to compensate the time of such consultants at least partly or to provide reasonable rewards to such consultants.

d. The "training the trainers" activities of KMCSN will also include training more people and organisations to offer the same free consultancy services to reach to more beneficiaries.

29. To better gather feedback and requirements from its members, other beneficiaries and supporting partners, KMCSN will also organise in-person, virtual and hybrid events when the needs arise.

a. Virtual meetings will be prioritised to allow wider participation, to reduce travel time/costs and also to better protect the environment.

b. In-person meetings will be considered for small group discussions if virtual meetings will be less ideal for the nature of the topic.

c. Hybrid participation will always be considered for any in-person meetings whenever possible.

30. KMCSN organises a Senior School Leaders Forum (SSLF), which are formed by appointed senior leaders of member organisations, such as leaders of school groups, school headteachers, school heads of a relevant area, and school board chairs.

a. Members of the SSLF shall be either individual members of KMCSN or staff of organisational members of KMCSN.

31. In addition to support its members, KMCSN will also actively encourage non-expert individuals such as parents and legal guardians, senior pupils, college and university students to be supporters, local champions, and non-expert helpers of KMCSN's activities.

a. A CyberChampions Scheme will be set up to facilitate management of such individual supporters and champions.

b. KMCSN's "training the trainers" activities will cover local champions who are interested in being individual members of KMCSN so that they can deliver cyber security and online safety education and awareness raising activities for children themselves and even train more other people to do the same.

Management, Operation and Governance

32. KMCSN will have an Executive Group (EG) chaired by iCSS's Outreach Lead (currently Professor Shujun Li, who is also the Director of iCSS). Other members will include Director of iCSS (if they are not the Outreach Lead), a rep from the STEM Hub, and a rep from KMCC (who can be Professor Shujun Li since he is chairing the Steering Group of KMCC), and one or more school reps.

a. Members of the EG are nominated by the relevant organisations and appointed by the Chair with consultation of all existing members of the EG.

b. Democratic election of school reps will be considered in the future, and such a decision will be made at an AGM of all KMCSN members.

c. The EG should meet monthly.

33. There shall be an Advisory Board (AB) representing more diverse voices within KMCSN memberships and non-members.

a. Around 1/3 of the AB shall be KMCSN individual members.

b. Around 1/3 of the AB shall be appointed representatives of its organisational members.

c. Around 1/3 of the AB shall be individuals who are not a member of KMCSN but have a substantial level of knowledge on pre-university cyber security and online safety education and

awareness raising. For instance, such AB members can be people from other regions of the UK or other countries, but working on a very similar course.

    d. The AB shall have a Chair, who is one of its members.

    e. The AB Chair shall be nominated by its members and appointed by the KMCSN EG.

    f. The size of the AB shall be between 6 and 20 to make it manageable.

    g. The terms of AB members and Chair will be decided collectively at the first meeting of the AB.

34. Organisations that do not meet the criteria of organisational memberships explained in Clause 13 can be partners of KMCSN.

    a. At this moment, iCSS/University of Kent is the owner/manager of KMCSN, so it is not considered a partner.

    b. The STEM Hub, CCCU, and KMCC are strategic partners of KMCSN as its co-founders.

    c. If KMCSN becomes an independent organisation or part of an independent organisation, iCSS/University of Kent will become a strategic partner of KMCSN as its leading co-founder.

35. KMCSN should have a dedicated website independent of iCSS, STEM Hub/CCCU or KMCC, and its own social media accounts. Such a website and social media accounts are managed by the EG or their delegates.

36. A newsletter can be set up to inform all members and other relevant stakeholders about activities and future plans of KMCSN. The newsletter can be made to allow non-member subscribers.

37. One or more mailing lists should be set up to facilitate communications between KMCSN to its members, among members of KMCSN and its different SIGs/SSLF.

    a. One main mailing list should be set up for KMCSN to communicate with organisational and individual members and CyberChampions of KMCSN.

    b. Two mailing lists should be set up for KMCSN to communicate with its organisational and individual members, respectively.

    c. A number of other mailing lists can be set up for different SIGs, SSLF, AB and other operational needs of KMCSN.

38. There shall be an Annual General Assembly (AGM) for all members of KMCSN to meet, review past activities and discuss future plans.

    a. The AGM shall be chaired by the EG Chair or their appointed deletage.

39. The Senior School Leaders Forum (SSLF) meets annually, and by default as part of the KMCSN AGM.

    a. The SSLF shall have a Chair, who is one of its members.

    b. The SSLF Chair shall be nominated by its members and appointed by the KMCSN EG.

    c. The size of the SSLF, terms of its members and Chair will be decided collectively at the first meeting of the SSLF.

40. The EG Chair or their delegate shall attend all AGMs, meetings of the AB and the SSLF, and are expected to give a report and answer questions from other participants.

41. All other members of the EG are expected to attend the AGM of KMCSN. In the rare case they cannot attend, they should send a delegate eligible to represent the corresponding organisation.

42. All other members of the EG are invited to meetings of meetings of the AB and the SSLF but their attendance are not required.

43. All meetings shall be held either virtually or allow virtual participation, in order to be more environmentally friendly and to accommodate people who cannot travel due to different legitimate reasons.