e-safety adviser
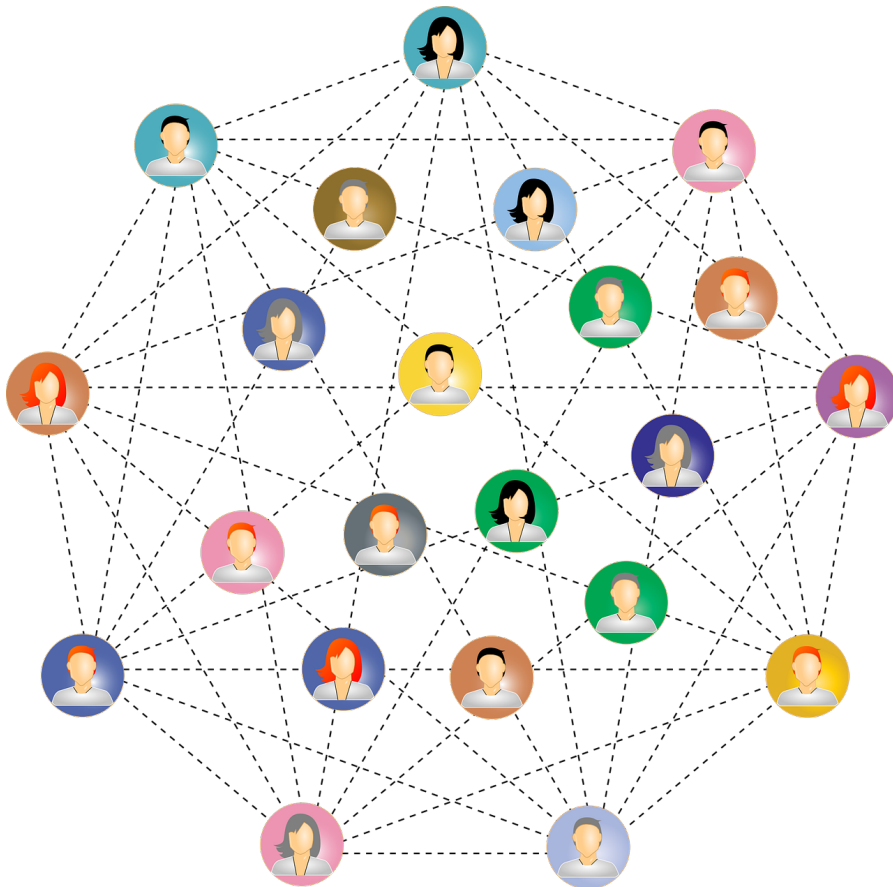
Online Safety Group

a guide to establishing your group, including roles and responsibilities.

Contents

The author

 I'm Alan Mackenzie. e-Safety, or to use the newer terminology online safety, has been a passion of mine for many years; I love technology and the huge benefits that can be realised through global connectivity and collaboration. I'm a strong believer that online safety is an enabler, not a showstopper. It should never be a barrier to innovative use of technology. It's about teaching users how to recognize, understand and mitigate risks in order that they can benefit from technology and reduce the likelihood of harm.

As the e-safety lead for a local authority, I became a CEOP Ambassador in 2007, which was a great starting point. In 2012 I became an independent consultant and since then I have worked with hundreds of schools, charities, commercial organizations, police and many others. Whether that's for training (staff, students, governors, parents), research, strategic initiatives, whitepapers, guidance and so much more, I love the diversity.

Most of all I love the challenges of empowering others in a world of technology where the future is a blank canvas.

Copyright

Contact Alan   📞 **01522 25 30 88**   ✉ **alan@esafety-adviser.com**

www.esafety-adviser.com

Introduction

Over the years the term 'e-safety' has taken on a whole new meaning and eventually became 'online safety' in early 2016 to take into account the wider range of risks and issues. Safeguarding children and young people from harm should always be the prime consideration, but it's clear that the issues have become much more widespread and therefore considerations for schools have expanded dramatically. Some of these considerations would include:

- The large majority of incidents will happen outside school but have a knock-on behaviour effect in school.

- Effective strategies to engage parents and the wider community - critical yet difficult and no single solution.

- Inspection considerations.

- Curriculum - just Computing?

- Evidence - what works, what could be improved?

- Standardized processes.

One person in school cannot hope to manage all of this, there is too much involved. There is little doubt that establishing a group with wide membership is one of the most forward thinking initiatives you can embark upon. But how do you go about it, who should be a part of it and what are the outcomes?

This guide has been put together to help you with these questions and more. Please understand it is a guide only, I'm a single consutant with no budget and these resources take a lot of time to put together, but if anything is amiss or you think anything could be included in future versions let me know.

Establishing your group

Before you start you need to decide what the outcomes of the group will be, and based on that who would ideally be in the group?

Step 1 - What are the outcomes?

What are you trying to accomplish and what are the benefits? Here are some examples:

- To draw upon the wide and varied knowledge of others with different skillsets, experience and opinions.
- To take into account and plan for new statutory requirements such as Keeping Children Safe in Education, ensuring that any new needs are met.
- To ensure there is a broad and balanced online safety curriculum, taking into account the needs and vulnerabilities according to age and other factors such as SEND.
- To monitor the impact of this curriculum, identify any gaps or weak areas.
- To plan for annual initiatives such as Anti-Bullying Week or Safer Internet Day.
- To spread the workload building resilience within the school.
- To monitor and review policy.
- To monitor incidents and ensure that they have been dealt with in accordance with school policy.
- To risk-assess any new technology in the school prior to purchase.
- To engage the school community - working together to benefit all.

Step 2 - Who should be in it?

The following is an 'ideal' list but you will need to tailor to your environment.

- Governor - ideally the governor with safeguarding responsibility.
- SLT representation.
- Computing Coordinator or Head of ICT plus PSHE Lead.
- Designated Safeguarding Lead.
- ICT technical support
- Pupils/students - school council or a chance to get others involved such as vulnerable students.
- Parents or carers
- Your neighbourhood PC or PCSO
- Representation from community groups such as scouts etc.

Step 3 - Roles and Responsibilities

It is recommended that roles and responsibilities are formalised in your online safety policy. The following are example roles to give you a starting point.

Whole-group responsibilities

- To review the online safety policy annually or in response to an incident.

- To monitor online safety incident log (note: not suitable for students to be present)

- To discuss training needs, including staff, parent/community awareness.

- To raise new community initiatives in response to training needs or as a result of polls/surveys.

- To coordinate annual events such as Anti-Bullying Week or Safer Internet Day.

Governor

- To independently chair the group, ensure minutes are taken and actions are delegated and actioned.

- Ensure that all initiatives, action points, concerns etc. are raised at Governors meetings.

SLT representative

- To ensure that training, education, initiatives, incidents etc. are in line with whole-school policy and strategic plan.

- To brief SLT on meeting minutes and any actions and/or concerns.

- Note: training (staff and governors) is constantly seen as one of the weakest aspects in schools.

Designated Safeguarding Lead

- Liaise with other agencies for any county-wide/national areas of concern.

- Retain responsibility for the online safety incident log (if you have one) alongside other safeguarding/child protection logs and ensure safeguarding incidents pertaining to online safety have been actioned accordingly.

ICT support

- To ensure that the group is kept fully updated with any network security incidents or areas of concern.

- To advise on the correct use and implementation of filtering categories to ensure age-related filtering is appropriate to education.

- To advise on other ICT aspects, e.g. monitoring requirements in line with Keeping Children Safe in Education.

Computing Coordinator, Head of ICT and PSHE Lead

- To review the online safety curriculum with other relevant members of staff, e.g. PSHE lead, ensuring that it is tailored to fit the needs of all students and statutory requirements.

- Keep up to date with new risks, issues, developments and resources in the area of online safety and brief the group accordingly.

Pupils/Students

- Pupils/students should be at the forefront of the group and any initiatives. It is important the school understands their concerns and their ideas as to how these concerns can be tackled. Opinions of students should be a primary focus; they can bring useful insights and experience to the group through meetings/polls/questionnaires with other students.

- Note: consider involving identified vulnerable students, for example those at elevated risk of harm.

Parents and carers

- Community issues and community voice ensuring advice and initiatives are spread far and wide in the community.

Neighbourhood PC or PCSO and community groups

- To bring to the attention of the group any incidents of concern or patterns of behaviour in the community.

- Helping to ensure advice and initiatives are spread far and wide in the community.

Keep staff, governors and parents up to date with online safety advice, guidance and opinion:

#DITTO is a FREE half-termly magazine in PDF format, full of information and guest posts which you can download and place on your own school website.

Sign-Up Online

http://www.esafety-adviser.com/latest-newsletter

Your first meeting

Your first meeting is all about setting the scene for the future and managing expectations. In other words, you will be setting the roles, responsibilities, standing agenda etc. so that everybody knows what their input is and importantly, the strategic purpose of the group.

1. Nominate a chairperson.
2. Discuss and agree on roles and responsibilities.
3. Decide standard meeting agenda (see page 14 for an example).
4. Agree on frequency of meetings and set dates for the year (e.g. termly, half termly).
5. Consider how information will flow into and out of the group.

Who will chair?

It is recommended that the governor chairs this group as he/she will already have a significant role at the school and will be fully aware of school processes/procedures.

How will the meeting notes be compiled and shared?

You may already have a process in place, for example the same process that you use with governors, commonly email, but there are other more collaborative ways that you could consider such as:

Microsoft Onenote
Google Docs (Google Apps for Education)
Evernote

** ** Whichever service you use, keep in mind Data Protection ** **

How often will you meet?

Everybody is busy so it's important that consideration is given to balancing the importance of such a meeting alongside the frequency.

In an ideal world I would recommend half termly meetings if possible. Or, you may wish to start off with termly meetings for the first year to see how it goes, and then revisit this after a period of time, e.g. 12 months. Also be clear that there may be a rare occasion when an extraordinary meeting needs to be held at short notice.

Furthermore, give consideration to the types of things that may be discussed at these meetings - it may not be necessary (or appropriate) to have students present due to the nature of the discussion, e.g. incidents.

Students could have their own meetings, e.g. with the school council, with outcomes of that meeting providing input to the e-safety group meeting.

What will you discuss?

The quality of the input will be a large factor in the quality of the output (see the input/output diagram), but what is important is that there is a structure to the meeting so that everything is consistently covered each time you meet, that everybody has a voice that is valued.

Commonly in any meeting there will be a standing agenda and 'any other business'. See page 14 for an example standing agenda.

Also don't forget there are standard times of year where you may have a specific initiative held annually, for example 'Safety Week'. There are also national initiatives that you should remember too such as:

- Safer Internet Day (February)
- Anti-bullying week (October)
- Christmas (think new consoles, games etc.)

Getting Information In

Group Members:

Governors and senior leaders

Designated Safeguarding Lead

Curriculum leads

ICT Technical Support

Students/Pupils

Online Systems

SWGfL Boost

Google alerts

Polls/questionnaires

Getting Information Out

Parents/Wider Community

Website and social media

School letter

Newsletter

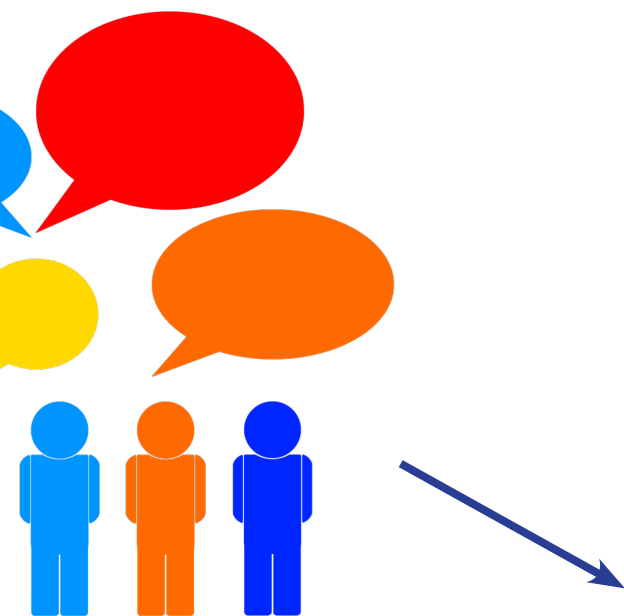Information evenings

Local media

In School:

Assemblies

Curriculum

eCadets, school council
or group representatives.

Staff meetings

Standing agenda - example

There will be standing items in each meeting which could include:

- Review and update of actions from last meeting.
- Review of online safety incidents - designated safeguarding lead.
- New natiional guidance or policy requirements - online safety lead.
- Filtering/monitoring reports - ICT tech support.
- IT security or data protection issues - ICT tech support.
- Concerns or questions from the community - parents, PC, PCSO.
- Updates on any in-process initiatives.
- Any other business - including proposals for new initiatives.

Other regular items may include:

- Anti-bullying week (discuss in July or September).
- Safer Internet Day (discuss in October).
- Annual review of online safety incidents (disucss in June/July).
- Discuss appropriate training needs as required (staff, governors, parents).
- Review online safety curriculum (discuss towards end of curriculum year to allow time for planning).
- Online Safety and acceptable use policies (reviewed annually or in response to an incident).

Community engagement

One of the most difficult, yet arguably the most important aspects of online safety is parental and community engagement, so you need to think out of the box, but in such a way that there isn't a significant amount of work to do.

Herein lies the beauty of the online safety group as certain responsibilities and initiatives can be devolved to other members of the group. Here's a small list of examples:

- Students - hold a weekly or fortnightly walk-in centre for other pupils (and parents?) to raise any concerns or questions.

- Curriculum - use the imagination and creativity of students to create a drama/play/rap etc. about certain aspects of online safety; there is no better way to get the parents involved. You could create a song or record a series of videos. These creative ideas not only inspire, but also pull in many other aspects of the curriculum so that you are not treating online safety as something which is bespoke.

- Newsletters - regular newsletters (e.g. #DITTO) with pertinent information discussed with the online safety group.

- Social media - don't be put off by some of the scaremongering stories you hear. There can be issues but the positive engagement hugely overwhelms the negative. Facebook is by far the best way of doing this with Twitter coming a close second, but there are plenty of others such as Pinterest and even Instagram. You could even use 2 or more for maximum engagement and these can be automated using a free service such as IFTTT (www.ifttt.com). See the Resources page on my website (www.esafety-adviser.com) for a guide to using Facebook as a school communication tool.

- The community members of your group (such as parents/carers, police, local groups etc.) are the best people to advise on getting this engagement message out.

Checklist for Online Safety Lead

In order to help you as part of your planning, here is a simple checklist that you can tailor within your group:

Create a document with a 'yes/no/in-planning' tickbox.

1. Online Safety policy reviewed with other relevant policies?
2. Acceptable use policies reviewed and appropriate according to age/need?
3. Planned online safety training/updates for all staff?
4. Internet filtering – differentiated and fit for purpose according to need?
5. Monitoring solution (if used) reviewed, risk assessment carried out and agreed with senior leaders/governors?
6. All previous incidents reviewed and appropriate actions taken?
7. Planned, embedded and progressive curriculum according to the needs of the students?
8. Reporting mechanisms in place and understood by all?
9. Risk assessments carried out, mitigation in place?
10. Appropriate and up to date information, supporting links and guidance available on school website?

Further explanation

1. Your online safety policy needs to be reviewed annually and endorsed by governors, unless there has been an incident, in which case you would review your policy to ensure that the correct processes were in place.

2. AUP's should be reviewed annually alongside the online safety policy.

3. KCSIE 2016 requires all staff (teaching/support) receive training (updates) regularly, which they have clarified as annually. We recommend you include within this training:

   • Any patterns of activity or incidents in the school and actions that have been taken.
   • Any changes to policy.
   • National updates in regards to trends, research, appropriate advice/guidance.
   • Code of conduct (professional boundaries) reminders to all staff.

4. Your internet filtering solution should be tailored such that traffic is filtered according to different needs (e.g. year groups, staff, volunteers).

CHECKLIST

5. KCSIE 2016 introduced a new requirement under 'filtering and monitoring'. Whilst there are technical monitoring solutions available (sometimes called behaviour management software that monitors activity on PC's, laptops etc.) schools should risk assess their own needs. For example, a small primary school with a single ICT suite, where all the PC monitors can be physically viewed by teaching staff may be a suitable monitoring solution.

6. It is important that any incidents, particularly those of a child protection nature, are reviewed to determine that appropriate actions have been taken, and if not they are followed up. For example, if a student has accidentally stumbled upon an inappropriate site/page, has this been reviewed with IT support to ensure that the filtering solution is working correctly?

7. Whilst 'eonline safety' is embedded within the Computing curriculum for most schools, it is recognised (and required by KCSIE) that this is embedded where possible throughout the curriculum, particularly PSHE.

8. Depending on your particular settings, there will be a variety of reporting mechanisms. It is important these are understood by all staff and students. Examples of reporting mechanisms might be:

- Worry box.
- School council/eCadets.
- School email address (e.g. anti-bullying – bullying@school.co.uk).
- CEOP reporting button on school website.
- Hotlines, e.g. Childline.

9. This refers to any new technologies you may be using in school. New technologies should be risk assessed against potential for harm to the child/adult and reputational harm to the school. A common example:

- School purchases new iPads. These can be used by class teachers to take photographs/videos of children to celebrate school achievements. Are these automatically backing up to iCloud? Are you happy with this? Has data protection been considered? Are these images/videos ever audited? Who has access? Are they taken home?

10. Ensure your online safety policy is online for others to view (particularly parents). You could also consider putting your acceptable use policies online too. Provide relevant, age-appropriate and up to date links on your school website to support and guide students and parents/carers, e.g. Childline/ NSPCC, Internet Matters, CEOP/ThinkUKnow, Anti-Bullying Alliance. Copies of DITTO magazine (ensure you link back to my website if you do this).

Risk assessing

What is Risk Assessment?

Schools have to risk assess all the time. Sometimes this is a formally documented process, sometimes it is assessment through experience. If you think about it, you are already risk assessing constantly: when you get into your car to go to work you take into account the weather, the amount of traffic on the roads, children waiting to cross the road and much more. This is assessment through experience. You know what to do in situations such as these. But, when something happens that is unfamiliar you have to re-assess and make a decision, you have to weigh up all the factors and the unknowns.

It's a matter of discussing all the unknowns and then coming up with a plan to mitigate against the risks. If you can't mitigate the risks, are they so low that you can accept the risk? This is where your e-safety group comes in.

Are you getting new technology in the school? Are you thinking of using a new service, perhaps a new cloud service or thinking about getting a Facebook page for parental engagement? All the members of your group have a part to play in this, for example your IT support will be able to advise on the technical aspects, parents will be able to raise any concerns from their perspective, the child protection lead will be able to raise or allay any CP concerns.

Liability

Risk assessment plays a very significant role in order to reduce the risk of harm to the child and adult but it also plays another vital role: to mitigate the risk of liability or damage to reputation of the school.

Whilst the purpose of this guide isn't to go into the different aspects of risk assessment, you can refer to Newsletter 12 for a more in-depth explanation, and my model e-safety policy for risk assessment templates, both of which are on my website at www.esafety-adviser.com

Useful links and resources

Further resources from Alan Mackenzie

All of my free resources are at - www.esafety-adviser.com

DITTO - free newsletters for parents and staff.

Model e-safety policy and guidance.

Questionnaires for staff, pupils and parents.

Twitter guide for teachers.

Using Facebook as a school communication tool.

...... and more

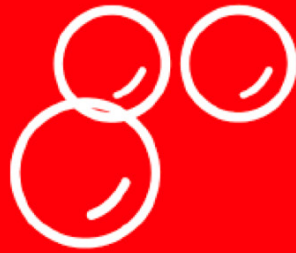## Other links and resources

Online training for staff and governors - http://www.theonline.academy

eCadets - empowering children - http://www.ecadet.zone/

Google alerts - http://goo.gl/emrm3Z

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

SWGfL BOOST reporting tool - http://boost.swgfl.org.uk/Home.aspx

Free self evaluation tool - 360Safe - http://www.360safe.org.uk

GoBubble

Safe social media for under 13s

1 CONNECTING THE WORLD'S CHILDREN

Step #1 — Teacher registers a school for free

Step #2 — Parent approves their child's account

Step #3 — Child connects with others the same age around the World

FREE for schools http://bubble.school

Contact Alan Mackenzie

📞 01522 25 30 88

✉ alan@esafety-adviser.com

🐦 twitter.com/esafetyadviser