



Online Safety Group

Copyright Notice

This guide and the course content is the sole copyright of SafeICT Consultancy Ltd (www.esafety-adviser.com) unless otherwise stated.

No part of this guide or the course content may be copied or distributed without express permission.

Table of Contents

INTRODUCTION	3
ESTABLISHING YOUR GROUP	4
Step 1 - What are the outcomes?	4
Step 2 - Who should be in it?	4
Step 3 - Roles and Responsibilities	5
YOUR FIRST MEETING	7
Who will Chair?	7
How will the meeting notes be compiled and shared?	7
How often will you meet?	7
What will you discuss?	8
GETTING INFORMATION IN	9
GETTING INFORMATION OUT	9
EXAMPLE STANDING AGENDA	10
COMMUNITY ENGAGEMENT	11
CHECKLIST	12
SUMMARY	14

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 effect in school.
- Effective strategies to engage parents and the wider community - critical yet difficult and no single solution.
- Inspection considerations.
- Curriculum.
- 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; treat it as a framework and mould into best practice within your school setting.

ESTABLISHING YOUR GROUP

Many schools will quite rightly state that there are already too many groups or meetings which all impact on curriculum and administrative time. There is no requirement to establish a completely bespoke group, it could be a sub-group of a committee or group you already have, e.g. a combination of your safeguarding group and school council.

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, advances in technology etc.
- 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 own setting.

- Governor - ideally the governor with safeguarding responsibility.
- SLT representation.
- Designated Safeguarding Lead / Child Protection Lead.
- Computing Coordinator or Head of ICT and PSHE 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 within your online safety policy. The following are example to give you a starting point.

Whole-group responsibilities

- To discuss new or developing issues, e.g. new apps children/young people are using, new games, emerging risks etc.
- 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 relevant 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.

Designated Safeguarding Lead / Child Protection 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.

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.
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 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 online safety group meeting.

What will you discuss?

The quality of the input will be a large factor in the quality of the output, 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 later in this document 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

Information to the group will come in a variety of sources, each of which will have valuable input to the group. This is the real value of a group such as this: different thoughts, ideas, opinions and experience.

For example, the DSL may become aware of an emerging concern through information shared by the local authority, e.g. the popularity of a new anonymised app which is being correlated to an increase in bullying incidents. Thoughts can be discussed by the group members, particularly the parents and students, to clarify if this is an issue in school and/or the community.

If this is an unknown, the chairperson could recommend a poll is carried out by the students to see if any further actions are required. If it is already clarified as an issue the curriculum leads could discuss a strategy to mitigate the risks and issues using the valuable input from students to ascertain what is most likely to work, e.g. an assembly, information sheets, advice and guidance for parents etc.

GETTING INFORMATION OUT

Getting the correct information out, in the right way, in a timely fashion is vitally important for success. Examples to be discussed amongst the group might be:

Parents/Wider Community:

- Website and social media.
- School letter.
- Newsletter.
- Information evenings.
- Local media.

See the Community Engagement page further on in this document for other ideas.

In School:

- Assemblies.
- Curriculum activities.
- Staff meetings (to keep all teaching and support staff up to date).

EXAMPLE STANDING AGENDA

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

- Review and update of actions from last meeting.
- Review of online safety incidents - designated safeguarding lead.
- New national 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 (discuss 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).

CHECKLIST

<input checked="" type="checkbox"/>	_____
<input type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input checked="" type="checkbox"/>	_____
<input type="checkbox"/>	_____

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 from www.esafety-adviser.com) 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. You could even use 2 social media services or more for maximum engagement and these can be automated using a free service such as Hootsuite or www.buffer.com.



CHECKLIST

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

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 2018 requires all staff (teaching/support) receive training (updates) regularly, which they have clarified as annually. I recommend you include within this training:
 - a. Any patterns of activity or incidents in the school and actions that have been taken.
 - b. Any changes to policy.
 - c. National updates regarding trends, research, appropriate advice/guidance.
 - d. 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).
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. A large primary

school or secondary school with different technology around the school would be a very different matter.

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 'online 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:
 - a. Worry box.
 - b. School council.
 - c. School email address (e.g. anti-bullying – bullying@school.co.uk).
 - d. CEOP reporting button on school website.
 - e. 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:
 - a. 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.

SUMMARY

I hope you have found this guide to be of some use; it takes into account many of the major frustrations I hear from schools such as:

- Time and resources.
- How do you know what you don't know?
- Parental engagement.
- Firefighting incidents rather than being pro-active.

It takes a little time to establish and get going, but I can't stress enough the benefits you will see if you plan and do this correctly.

I can't cover everything. If you feel anything has been omitted, or if you have examples of best practice within your setting please do let me know so that I can share this with others.

Alan Mackenzie

www.esafety-adviser.com

Twitter: @esafetyadviser

