

Using Social Media and Technology in Educational Settings

Considerations, guidance and risk assessment templates for schools and educational settings considering the use of Social Media



Kent County Council e-Safety Strategy Group - September 2011

Second Edition - October 2011

Disclaimer

Kent County Council (KCC) makes every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable. Nevertheless, KCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication. This document is provided as guidance only and it is recommended that schools seek further guidance or legal advice if they have any concerns regarding the specific legal obligations in response to questions raised by this document.

The copyright of Kent materials is held by Kent County Council. However agencies that work with Children and Young People are granted permission to use all or part of the materials for not for profit use, providing the KCC copyright is acknowledged and we are informed of its use.

Using Social Media and Technology in Educational Settings

The Kent e-Safety Strategy Group comprises multi-agency professionals from across the Kent children's workforce to help professionals, schools and other settings make informed and appropriate choices about using social media tools. This document aims to help schools and educational settings consider safe practice in order to protect staff, pupils and the wider community.

Social media tools can include websites such as blogs, Wikis, social networking and video sharing sites. Sites such as Facebook, MySpace, Twitter, YouTube and Flickr have become everyday forms of communication for both adults and children. Whether accessed through a computer or mobile phone, they help us stay in touch with friends and family members, share photos, watch videos, play games and even organise events and campaigns.

However social networking and media sites can have risks. They have changed how we communicate and this can lead to people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and abuse children. The boundaries between the "real" world and the "virtual" can become blurred and this can have potentially serious consequences for staff, parents/carers and children who may not be aware of the risks behind everyday online activity.

Online social media tools can also be excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with pupils and the wider community. The positive use of social media and Information and Communication Technology (ICT) within schools and settings for curriculum and learning is encouraged. However it is essential that their use is carefully considered in advance, in order to ensure all members of the school community are kept safe.



Safe Use Considerations for Schools and Educational Settings

The use of technology and social media tools in the classroom is a school/setting decision and should where possible be based on a risk assessment approach. The benefits of using the tool/technology should significantly outweigh the concerns and schools and settings should be able to clearly demonstrate the steps they have taken to reduce any risks identified.

Good e-Safety practice should be fully embedded across the establishment before schools and settings consider using Social Media tools. Best practice includes up-to-date and appropriate training for every member of staff, as well as pupils, parents and carers. Schools/settings should have a designated e-Safety lead and an up-to-date e-Safety Policy.

The decision on using Social Media tools should be made as a school/setting and requires the full support and backing of the Senior Leadership Team and Governing Body. Schools are advised to risk assess the use of Social Media tools prior to use as part of the schools legal duties to comply with The Children's Act 1989, the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999 which makes it clear that all schools have a duty of care to ensure the safety and well being of pupils and staff. The setting's behaviour and complaints policies may also need to be checked. The school/setting will need to be aware of their responsibility to moderate content and to ensure that the content is kept up to date. Use must also be in accordance with the sites terms and conditions.

Schools and settings should always be mindful that, due to the global nature of the internet and the speed at which technology moves, online tools can very quickly change and content can be distributed much further than intended. Risk cannot be 100% removed from any site or service so a clearly defined incident procedure is essential.



Schools and settings should have clearly defined policies in place which specify when and how social media and related devices (e.g. mobile phones) will be used. Considerations about general safe use in the classroom may include:

- Supervision in the classroom with technology must be appropriate to the children's needs and abilities. It is recommended that primary aged pupils should always be supervised by a member of staff. Internet searches and online activity with KS1 children should always be pre-checked and teacher led. Age-appropriate search engines should be used by KS2 pupils and websites should be pre-checked by the teacher. Supervision in the secondary school will vary according to the pupils' understanding and ability. KS3/4 students should be taught age appropriate behaviours and safe searching techniques to support their learning.
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot be relied on alone to safeguard children.
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks.
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online.
- All pupils and staff should understand how to critically evaluate online content.
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the Senior Leadership Team.
- School/setting provided devices and tools should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than staff personally owned equipment.



Considerations to make before using Social Media technology



It is essential that the correct tool is selected for the purpose or aim of the project. For example, to communicate with parents and carers about school based decisions, it might be better to use a blog to enable a discussion rather than a Twitter page as this only allows for a limited amount of interaction. Schools and settings should preferably use tools available on their official school/setting website or Learning Platform as will be more likely to offer a more controlled environment.

Central to selecting the appropriate Social Media tool or technology, is deciding who the target audience is (parents/carers, staff or pupils etc) and what purpose it will serve. When targeting parents, schools and settings will need to be aware that not all families will have access to the internet at home. To combat this issue some establishments have offered open evenings to families or have an internet enabled computer in an accessible location for parents/carers to access after signing an Acceptable Use Policy. It is also important to find out if your audience would like to engage via social media, for example some students may not wish to add their school/setting on a social networking site!

It is important that schools and settings are aware how Social Media sites function and are aware how to make them as safe as possible, before use. This might include understanding how to make profiles “private” or using groups or pages or feeds to engage with the community instead of individual profiles. (See “further advice and guidance” for links on how to achieve this)



When using Social Media with children, schools and settings should be aware of site age restrictions and should only use sites that are deemed to be age appropriate and suitable for educational purposes. Staff should carefully check the Terms & Conditions of any websites used in the classroom carefully as Schools and settings should be careful to not promote or advocate the underage use of any sites. (See “further advice and guidance” for links on how to achieve this)

Social Media tools may need to be moderated and regulated by the school according to the age of the children. It is important to be aware that very few social media tools are able to verify and authenticate users appropriately, unless the system is controlled directly by the school/setting or by a subscription service. Examples of sites which authenticate users may include the schools learning platform, Kent Learning Zone, Ning, ELGG, Edmodo, Super Clubs, RadioWaves etc.

Where possible, when using services which the school cannot control via moderation or user authentication (e.g. Facebook, Twitter, YouTube), it is recommended that comments etc. are moderated or approved before they are made live and membership to online groups etc is controlled (e.g. people must request to join a group or follow) by the school/setting. (See “further advice and guidance” for links on how to achieve this)

All members of staff must be aware that, due to the ease of publishing information and content online, it is now very easy for staff to confuse writing in their capacity as a member of staff with sharing their own individual opinion. Staff must be aware that even as an individual, his/her actions could be criticized and seen as bringing a school into disrepute, especially if other users are aware of their role. This may have disciplinary, civil or even criminal consequences. It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff should always remember that once content is shared online it is possible for it be circulated far wider than intended without consent or knowledge.

In order to protect staff, it is strongly recommended that separate professional accounts, pages or profiles should be used when communicating with pupils or the wider school community. This should be supported and approved by the Senior Leadership Team. Establishment approved email addresses and contact details should be used and staff should be very careful not share any personal contact details or information with pupils (past or present) or their parents/carers. Staff must also be aware that their duty of care to pupils will still apply when using online tools and there should be procedures in place to support staff with this. (See “further advice and guidance” for links on how to achieve this). This should be clearly reflected in the settings Acceptable Use Policy when members of staff are using social media tools to communicate with the school community for professional purposes.

It is recommended that schools and settings should complete a risk assessment for the communication tool/site/technology prior to its use in the classroom as part of their legal duty of care towards pupils. In a recent report published by Ofsted in September 2011 “Safeguarding Schools:best practise” it was noted by Ofsted that a common weakness found in schools judged to be inadequate, was that they failed to carry out robust risk assessments. Ofsted felt that schools judged to be Outstanding were common in their approach to their safeguarding responsibilities and that “outstanding” schools:” ...comply with requirements and often move beyond them; it is not seen as a burden but as a reasonable and essential part of the fabric of the school; it pays attention to the meticulous and systematic implementation of policies and routines; it involves every member of the school community in some way; and it has a sharp eye on the particular circumstances and needs of all pupils, especially the most vulnerable.” For more information on this report, please see the Further Advice and Guidance section.

There is no such thing as 100% safe, so staff must know what to do to reduce the online risks. Staff must fully understand how sites work and what different settings or functions are available to use. (See “further advice and guidance” for links on how to achieve this)

Establishments should evaluate online communication projects to explore successes or problems. It is important to understand what the goals of the project are and what any successes will look like and to set a realistic timescale for evaluation. If the school is using a communication tool then it’s recommended to begin with a smaller focus/pilot group before rolling out the project across the school/setting. If the project has been successful then this should be celebrated by the school/setting and built upon. If the project has not succeeded, then the school/setting should consider why and what (if any) changes could be made to move the aims forward.



Checklist for using Social Media Tools in Educational Settings

Before using any Social Media tool, schools and settings might like to consider the following:

- What are the objectives/outcomes for this project?
- What do you want to communicate?
- Who is the intended audience (if using a communication tool)?
- Have you surveyed your audience to find out if they will engage with the tool?
- Why do you need to use this technology over traditional methods of communication or learning?
- What is the most suitable medium/site to use for this purpose and why?
- Will the project be student, parent/carer or staff led?
- Have you risk assessed the site to identify any safety concerns? If so, what changes will or can you make to reduce these risks?
- Has the site been risk assessed by both educational and technical staff?
- Do the Terms and Conditions allow you to use the site in the classroom or for your required purpose?
- Is the site age appropriate?
- Do you have parental consent (if necessary)?
- Do you have appropriate permissions or consent for any images, documents etc. to be shared?
- Have you explored the sites privacy and control settings?
- Can you restrict access to only your intended audience for all or part of the site (essential if sharing information you wouldn't share publicly)?
- Does the tool offer moderation? If so, who will be responsible for moderation on a regular basis?
- Do you have the resources (people, time etc.) to support this activity?

- Is use of social media covered in the School/Setting e-Safety Policy?
- Has the e-Safety Policy been updated recently and has this been communicated to all members of the school community?
- Have you created or adapted your Acceptable Use Policy to reflect your use? Has these been signed and created for all those involved (this is essential if using a communication tool)?
- Does the school/setting have clear rules/boundaries about safe and appropriate online behaviour and has these been communicated to all those involved?
- Have all members of the community received up-to-date training on e-Safety?
- Are the Senior Leadership Team involved and aware of the use of Social Media?
- Do you have documented approval and consent from SLT?
- Are you preparing a pilot project first?
- How will you evaluate the success of the project?



Risk Assessing Social Media tools



Risk assessing websites and tools is a useful way for schools and settings to develop safe and appropriate practice in the classroom and help to protect staff and students.

Risk assessments can be carried out prior to using any tool or technology in the classroom and it is good practice for schools to risk assess social networking tools before using them for an educational purpose.

When carrying out a risk assessment it is recommended that:

- The risk assessment should be carried out by both technical and curriculum focused members of staff.
- The published policies for a new service should be evaluated for privacy and data security (e.g. minimum age) and the site's user interface should be tested e.g. how to delete and block accounts and moderate content. It is important for schools to understand what personal data is collected, how it is used and whether there is an audit trail that can be traced back to a real identity.
- The impact of introducing a high bandwidth service on to a network should be evaluated.
- The content e.g. the suitability and reading age of any advertising or content should be assessed.

Two sample risk assessment templates are provided for schools to use and adapt.

Risk Assessment Template for the use of Web Tools and Technology in the Classroom

Site/Service:	
Brief Description of Service:	
Purpose:	

Summary of Risk Assessment Decision

Risk	Staff	Early Years	KS1	KS2	KS3	KS4	16+
General							
Privacy, Data Security							
Content Suitability and Age limits							
Communication							
Filter site?	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N

Key Issues and Action Required

Risk Identified	Action Taken	Action by	Date

Risk Assessment Checklist

Carried out by:

Role:

Date:

	Yes	No	Further information
General Considerations			
Endorsed by recognised authority for education use			
Service has good reputation for dealing with concerns			
SLT Approval			
Documented in School Policies and procedures			
Whole School e-Safety training provided			
Privacy and Data Security			
Registration of users required?			
Anonymous registration possible?			
User posts attributed to real, verified identities?			
Service can be administrated by staff			
Minimum age is suitable for the setting?			
Privacy tools			
Personal Data Collected – Logs Data			
Personal Data Collected – Email Address			
Personal Data Collected – Address/Phone numbers			
Personal Data Collected – IP Address			
Personal Data Collected – Cookies (Sessional or persistent)			
Personal Data Collected – Data sharing with other services			

Content Suitability			
High Bandwidth – Internet radio/TV			
High Bandwidth – Internet telephony			
High Bandwidth – File sharing			
High Bandwidth – Personal Storage			
High Bandwidth – Streaming Media			
Adult Material			
Advertising Material			
Dating/Personal			
Weapons			
Promotion of drugs, alcohol, tobacco etc			
Promotion of violence, hatred, racism etc			
Promotion of gambling			
Promotion of extremist organisations			
Promotion of Illegal Activity			
Promotion of computer misuse			
Other inappropriate content			
Communication			
Moderated by CRB Checked Adult			
Teacher/staff admin controls			
Age banding/tools provided			
Communication between pupils (within school)			
Communication between pupils (outside of school)			
Child to teacher communication allowed			
Unverified users present			

Risk Assessment Template for the use of Web Tools and Technology in the classroom

Date:	Assessed by:	Checked / Validated* by:	Website/Technology:	Audience:	Review date:
Purpose:					

	Hazard	Who might be harmed and how	Existing measures to control risk	Risk rating	Result and actions needed to be taken
Age Restrictions					
Membership verification					
Privacy/Profile Settings					
File Uploads					
Collaborative Tools					
Search Options					
Content and Design					

	Hazard	Who might be harmed and how	Existing measures to control risk	Risk rating	Result and actions needed to be taken
Advertisements					
Content Ownership					
Adult Content					
Moderation of site					
Safety					
Report abuse or content					
Privacy Policy					
Terms of Use					
Deleting and Controlling accounts					
Parental Consent					
Other					

Action Plan for the use of Web Tools and Technology in the classroom

Date:	Assessed by:	Checked / Validated* by:	Website/Technology:	Audience:	Review date:
Approved by:					

Action plan:				
Hazard	Further action required	Action by whom	Action by when	Done

Further Advice and Guidance for Educational Settings

- Kent Schools and settings can consult with the e-Safety Officer to discuss ideas and options before using social media tools or technology via: esafetyofficer@kent.gov.uk or 01622 221469. Training is available via EiS: www.eiskent.co.uk, CPD Online <http://cpdschools.kenttrustweb.org.uk> and KSCB www.kscb.org.uk
- Ofsted have published a report in September 2011 “Safeguarding in schools: best practice” which illustrates and evaluates the features of best practice in safeguarding, based on inspection evidence from the 19% of all maintained primary, secondary and special schools, residential special schools and pupil referral units inspected between September 2009 and July 2010 where safeguarding had been judged outstanding. It also draws on a more detailed analysis and evaluation of safeguarding practice in a small sample of outstanding schools visited by Her Majesty’s Inspectors and highlights some examples of recommended e-Safety practise and highlights the importance of completing risk assessments as part of all safeguarding procedures. <http://www.ofsted.gov.uk/resources/safeguarding-schools-best-practice>
- “Safer Use of New Technology” is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety
- Childnet International has also considered using Social Networking sites to engage with young people and the community and have identified positives and risks with the most common tools. The results can be found at www.digizen.org/socialnetworking/
- “Supporting School Staff” is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: www.digizen.org/resources/school-staff.aspx
- The UK Safer Internet Centre Professional Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.
- Teach Today is a useful website which provides useful advice and guidance for staff from industry: <http://en.teachtoday.eu>
- 360 Degree Safe tool is an online audit tool for schools to review current practice: <http://360safe.org.uk/>

- Documents are available to support schools in safely using social media tools. Yorkshire and Humber Grid for Learning (YHGfL) have produced a series of helpful guidance documents for schools and staff around the safe use of Facebook. Currently these documents can be accessed at www.yhgfl.net/eSafeguarding/eSafety/Safer-Internet-Day-2011
- Guidance for specific popular services:
 - Facebook:
 - The Facebook safety centre includes advice and guidance for teachers (as well as parents, teenagers and law enforcement) which can be found at www.facebook.com/safety
 - Facebook has created a set of guidance for educators which may be useful to Secondary Schools considering the use of Facebook within the classroom: [http:// facebookforeducators.org](http://facebookforeducators.org)
 - The Facebook Help Centre includes commonly asked questions about the safe use of Facebook as well as other concerns and queries www.facebook.com/help
 - Facebook have published a guide to help users consider their online security and privacy which can be found at: www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf
 - YouTube provide Help and advice for educators via the Google Help Centre: www.google.com/support/youtube/bin/answer.py?answer=157105
 - Twitter help and safety information can be found at <http://support.twitter.com>

Acknowledgements

This document has been the work of the Kent e-Safety Strategy group, including: Rebecca Avery, Families Social Care, Kent County Council; Peter Banbury, ICT Commissioning, Kent County Council; Justine Croft, Connexion Kent and Medway; Janet Davies, Libraries and Archives, Kent County Council; Alan Day, ICT; Tracey Tee, Petham Primary School; Rachel Keen, SENICT; Steve Moores, Maidstone Grammar School; Mike O'Connell, Families and Social Care, Kent County Council; Godfrey Pain, Kent Police; Lindsey Prestage, Libraries and Archives, Kent County Council; Carol Webb, Invicta Grammar School; and Suze Youde, Kent Youth Service, Kent County Council.

Additional comments have been made from Ruth Hammond, 2RH Education and Will Gardner, Childnet International.

With thanks to material adapted from resources by CEOP (Child Exploitation and Online Protection Centre), South West Grid for Learning (SWGfL), Yorkshire and Humber Grid for Learning (YHGfL) and Childnet International.

Please visit www.kenttrustweb.org.uk?esafety to download additional copies.