Frequently Asked Questions for Educational Setting Leaders about Using Social Media

Why do educational settings need to consider using social media tools?

In today's modern society, social media is often considered to be an everyday communication tool. For many members of our school communities, social media is the most commonly used communication channel; it's how people stay in touch with friends and family, but also how many people access local and national news or events. Schools, nurseries, playgroups and youth groups are increasingly turning to popular social media tools to increase their engagement with their wider community, for example, to communicate news and events with parents/carers.

In some cases, educational settings may prefer not to have an official social media presence; however, many are finding that this is no longer a choice. For example, some popular social media sites automatically create accounts based on local interest, so you could find that a Facebook page may have been created for your setting after a parent or member of staff has listed themselves as either working at or visiting the site. Additionally, many educational settings are finding that members of the community (such as parents) are creating unofficial profiles to communicate and network locally, e.g. Parent Teacher Associations (PTAs) and friends associations. In some cases, social media is used as a platform for the community to share their views or experiences.

For many parents, their first step when making a decision about their child's school or nursery place will be to consult the internet, using an online search tool such as Google and the school website. The Ofsted Common Inspection Framework highlights that Inspectors will also explore content shared online about the school or setting, pre-inspection. Your official website is likely to be the first place visited by people trying to find out about your school/setting, but their online searches may also direct them towards unofficial or unmanaged channels such as Mumsnet, Facebook and local and national online news sites.

Educational settings cannot respond effectively to positive or negative content posted online if they don't know what is being posted about them! Additionally if educational settings are not actively engaged in developing or managing their social media presence then they may find it difficult to implement strategies to safeguard all members of the community or to respond effectively to issues if they occur.

A well-developed, responsive and managed online presence will enable schools and settings to develop an effective strategy to engage and connect with current and prospective members of the community. It could now be suggested that it is no longer a case for education settings about "if" they use social media but more of a case of how well they use social media.

What are the risks of using social media for educational settings?

Social media users are likely to encounter a range of risks online, which can be categorised as content, contact and conduct. The potential risks associated with official social media have been summarised in these categories below:

	Commercial	Aggressive	Sexual	Values
Content	Inappropriate advertising Spam Copyright Hacking Pressure on school/setting ICT systems e.g. bandwidth demands	Violent content being shared Unwelcome hateful comments	Pornographic content being shared Unwelcome sexual comments being made	Bias Racist and extremist content Misleading info/advice Distressing or offensive content being posted/shared
Contact	Members of the community being identified e.g. due to images or locations being shared publically Harvesting data Sharing personal information	Staff or members of the community being bullied, harassed or stalked	Children or vulnerable adults meeting strangers Sexualised bullying (including sexting) Grooming and Online Child Sexual Exploitation	Self-harm and suicide content being shared Grooming for extremism
Conduct	Hacking Privacy and confidentiality breaches Copyright	Staff or members of the community being bullied, harassed or stalked	Members of the community creating and uploading inappropriate or illegal content Sexualised or harmful behaviour (including peer on peer abuse)	Members of the community providing misleading information and advice; encouraging others to take risks online; sharing extremist views Problematic Internet Use or "Addiction"

Content adapted from EU Kids Online 2008

Another consideration, when using social media as a communication approach, is that not all members of the community use the same tools; this could lead to some members of the community being isolate and missing out on vital information. Therefore, social media should not replace traditional communication routes; it should form part of the wider communication strategy. Educational settings should ensure that content is made available in a variety of formats and locations, such as: official websites, newsletters etc.

Educational settings need to identify the range of potential issues that could affect their community before using social media tools, and leadership need to demonstrate that they have taken reasonable and appropriate action (where possible) to reduce these risks.

Do I need a social media policy?

If educational settings are using social media as an official communication tool, then clear guidance will be required to ensure that they are not exposed to legal risks and that their reputation is not adversely affected. A social media policy should explore a range of

concerns and identify clear procedures to help reduce risks, respond to concerns and ensure that all members of the community are safeguarding from harm (both on and offline).

Even if settings do not use social media officially either as a communication channel or with learners, then it is recommended that appropriate guidance is in place to safeguard all members of the community. Keeping Children Safe in Education (KCSIE) 2016 highlights that schools and colleges must ensure that their staff behaviour policy (sometimes called the code of conduct) covers communications including social media.

Managers, leaders, Headteachers and Safeguarding Leads should explore the range of benefits and risks to ensure that a proportional and realistic policy decision is made; where possible, parents, children and staff should be included within this process in order to increase engagement and develop whole setting ownership of the policy.

Kent County Council provide a template social media for schools and settings to adapt within the online safety policy template: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

Is there a way that I can find out if content has been posted about my school/setting online?

One of the first places to start reviewing your online presence is through popular search tools, such as Google or Bing. Leaders and managers should carefully consider the results and be sure to check results beyond the first page.

There are also a range of tools available to help leaders identify content posted online:

- 'Google Alerts' is a way to keep track of public content posted online about your school/setting. Leaders can set up an alert for any key words, phrases or names and can opt to receive an automatically generated e-mail (immediately, daily or weekly), whenever that content is posted online. www.google.com/alerts
- Content management tools such as "Hootsuite" and "Tweetdeck" (other tools are also available) constantly search social media channels for keywords such as names and "hashtags" and can be used to manage social media content. These tools will need a member of staff to login to access search results.
- There are also paid services which can scan for keywords etc. such as, the reputational alerts tool within South West Grid for Learning's 'Boost': https://boost.swgfl.org.uk/

Leaders should ensure that all members of the community are aware of what is considered to be appropriate online behaviour. Pupils, parents and staff should feel able to use existing reporting procedures, such as speaking to the Designated Safeguarding Lead (DSL), to share concerns about content posted online.

It is also important to note that leaders cannot force staff or members of the community to befriend them online so they can monitor the content being posted. This could, in some cases, be viewed as unlawful and may leave leaders vulnerable to allegations and criminal, civil or disciplinary action.

Can't we just ban our community from using social media or posting content online about us?

No. An attempt to ban learners, parents or staff from using social media in their own personal time is going to be unrealistic, unreasonable and unenforceable. This approach is likely to create a culture of mistrust and secrecy which could, in many cases, increase the risks posed on social media by the community; people may hide their activity or not report concerns for fear of punishment or sanctions.

It is important to recognise that members of our community, and indeed the wider public, are entitled to hold opinions. Whilst many of their comments will be positive, some might not be so pleasant; it's important to remember that expressing these views is not always illegal or preventable. Leaders should seek to build a positive online presence and engage proactively with the community to minimise the possible risks.

The best approach is to promote a transparent relationship throughout the community and for leaders to be actively engaged and role model positive social media use.

How do I know which social media tool to use?

The central consideration when selecting the appropriate social media tool or technology should be the target audience (parents/carers, staff or pupils etc.). Educational settings should first consider using tools available on their official website or Learning Platform, especially when working with learners as this will offer a more controlled environment.

When targeting parents, educational settings will need to be mindful that not all families will have access to the internet at home. To prevent those families feeling excluded or isolated, some educational setting will need to offer open evenings for 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 parents may not use all types of social media and many learners may not wish to add or follow their school or college via their personal social networking site!

Once you have taken these factors into consideration, there is a vast range of popular social media tools available. It is essential that the correct tool is selected based on the purpose or aim of the communication. For example, to generate a discussion with parents and carers about educational setting decisions (such as when updating policies) then it might be better to use a blog, as this allows users to interact more.

It is important that educational 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.

I don't understand how social media works- do I have to use it?!

Senior leadership must be aware that the ultimate responsibility for online safety and the safe use of technology (include official use of social media) lies with them. If leaders do not understand social media tools then it's unlikely they will be able to make informed decisions regarding safe use by their setting and may be unable respond appropriately to potential concerns.

Many leaders choose to set up social media accounts, with the intention of simply learning how certain tools operate and exploring the possible risks, in order to develop a comprehensive risk assessment. They then de-active or delete the accounts or sites after use. Some educational setting leaders may also choose to have a social media account with the sole aim of using it to report concerns online.

It is essential that leaders spend sufficient time getting to know how sites work, before creating official accounts and using them with the wider community. Leaders must fully understand the different settings that are available, including report mechanisms and privacy options.

Additional guidance with regards to Facebook Pages, Facebook Groups, Twitter and YouTube can be found within Annex H, I, J and K.

What should I do if a member of the community posts something negative online about my school/setting?

In some cases, content posted online can and simply be ignored. In some situations just knowing that the content exists online enables leaders to prepare responses in case further concerns are raised.

If you do choose to take action, then it is important to ensure that the response is proportionate and balanced. The initial response must be led by impartial decision and not by personal emotions; this can sometimes be difficult, especially in cases where the comments are intentionally hurtful or untrue. Leaders must be aware that over-actions can sometimes inflame situations further and could result in a breakdown of trust and relationships.

If you find that negative content has been posted by a member of the community, the best response is usually to speak with the person concerned as soon as possible; ideally this conversation will occur face-to-face. There is specific guidance for leaders regarding responding to complaints made on social media on Kelsi: http://www.kelsi.org.uk/school-management/complaints

If the content is posted by unknown individuals (e.g. people not known to the community) or anonymously, such as comments posted on local news website, then best approach is to report the concerns directly to the website involved. Most websites will have help sections and report mechanisms. It's also a good idea to look at website's terms and conditions; many forums will have community guidelines which set out appropriate behaviour online, which can be helpful to reference when reporting concerns.

In cases where negative comments are posted on the official social media channel, then you may need to consider whether the content raises a legitimate and valid concern or complaint. If so, it may be appropriate to contact the person directly, ideally in person, and direct them towards the official complaints procedures; you may choose to make these available on your website. If the content contains offensive language, etc. you may choose to simply remove the content and contact the person who posted the content to explain why you took this approach; you may also wish to post a more general response about the wider topic, explaining the official position and directing the community towards the official complaints procedure.

It is advisable that leaders save copies/ screenshots of negative comments or concerns posted online, as well as recording direct URLs (specific web links), times, dates, locations and names of those involved; this may be required as evidence should further action be required either now or at a later stage. (NB do not copy content which could contain indecent images of children).

If people are persistently posting negative content on official social media accounts, then you may choose to block or unfollow the account concerned. In some cases, if the behaviour breaches the sites terms and conditions or community guidelines, you can also report the account to the social media provider.

Some negative comments posted online could be considered to be a criminal offence, if they contain credible threats or extreme hate (such as racism or homophobia); in these cases, the Police should be contacted immediately.

If an allegation is being made against a member of staff, leaders must ensure they follow the Local Authority allegations procedures.

Leaders may also find it helpful to access guidance and support available from their union and also the Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Kent educational settings may wish to seek further advice from the local authority, including the Education Safeguarding Team, Area Education Officer (AEO), Local Authority Designated Officer (LADO) and Schools Personnel Service (SPS).

How can my educational setting make the use of social media safer?

There is no such thing as 100% safe, so leaders must take appropriate steps to reduce and manage online risks. It is recommended that educational settings complete a risk

assessment for the communication tool/site/technology prior to its use in the classroom. Annex C may be helpful for leaders to document decision making.

A key area to explore will be the website or app's terms and conditions, as this will highlight some important issues to consider, for example:

- What are the app/site age restrictions?
    - Only use sites that are deemed to be age appropriate and suitable for educational purposes.
    - Be careful to not promote or advocate the underage use of any sites.

- Does the app/site collect personal data? If so, where is it held?
    - Ensure the use of the app/site is in accordance with the schools legal obligations as per the Data Protection Act 1998

- Do you have appropriate consent from stakeholders?
    - Ensure you have appropriate written consent for sharing photos/videos
    - Ensure you have appropriate consent or licenses for sharing any images or music not created by the school

- Who will be responsible?
    - Consider who will be responsible for managing and uploading content
        - (NB be aware that ultimate responsibility will sit with the Headteacher)
    - Ensure the relevant policies (including Acceptable Use Policies) up-to-date and reflective of social media use to ensure social media tools are used safely

Social Media tools may need to be moderated and regulated by the educational setting 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 educational setting or by a subscription service.

When using services which the educational setting cannot control via moderation or user authentication (e.g. Facebook, Twitter, YouTube), it is recommended that comments etc. are screened 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 educational setting.

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

Additional guidance with regards to Facebook Pages, Facebook Groups, Twitter and YouTube can be found within Annex H, I, J and K.

How can leaders, managers, Headteachers and Designated Safeguarding Leads enforce the Social Media policy with staff?

KCSIE 2016 highlights that schools and colleges must ensure that their staff behaviour policy includes the appropriate use of technology. Educational settings should therefore implement an appropriate Acceptable Use Policy (AUP) which clearly states expectations for safe use of social media, both officially and personally, as well as any sanctions for staff misuse. Kent County Council provide a template AUP for schools and settings to adapt www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

This policy should be supported with up-to-date, regular and robust staff training, as part of induction and child protection training; online safety training should be provided for all members of staff at least annually. Effective training will ensure that all members of staff are aware of the risks associated with using technology and social media and have appropriate understanding and ownership of policies in order to safeguard both themselves and children.

In order to protect staff and maintain professional boundaries it is strongly recommended that separate professional accounts, pages or profiles are used when communicating with pupils and the wider community for professional purposes. This activity should always be supported and approved by the Leadership Team. Educational setting approved email addresses and contact details should also be used and staff should be very careful not share any personal contact details or information with learners (past or present) or their parents/carers.

Staff must be aware that their duty of care to learners will still apply when using online communication tools and procedures should be in place to support staff with this; which should be clearly reflected in the educational settings Acceptable Use Policy.

Staff need to be aware that even as individuals, their actions online could cause the school to be criticised, or bring the school into disrepute; this may have disciplinary, civil or even criminal consequences.

When publishing information and content online, it is crucial that all members of staff are aware of acceptable behaviour, boundaries and professional practices. Staff should be careful not to obscure their official capacity as a member of staff at the school by sharing their own individual opinion on official school pages. In order to protect their professional reputation and status, staff should also be reminded that once content is shared online, it can be circulated far wider than intended without consent or knowledge.

The Kent County Council Online Safety policy template and Acceptable Use Policy Template contains further information regarding staff and social media: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

Can staff use their personal equipment to post social media content on behalf of the educational setting?

We would strongly advise against the use of staff using any personal equipment or devices to access social media or post content on behalf of the educational setting.

Allowing staff to use personal devices on site is likely to undermine the wider safeguarding culture within a setting; this can lead to inappropriate behaviours being unchallenged and create opportunities for offenders.

Additionally, if personal devices are being used to take images of children, there is an increased likelihood of allegations being made against staff and possible breach of date protection regulations.
Many educational setting are now providing staff with officially provided equipment to access official communication channels as this means that protection is significantly increased for both children and staff.

The Kent County Council Online Safety policy template and Image Use Policy contains further information regarding taking images and the use of mobile phones and personal devices: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

Can educational settings share images of learners via social media?

Educational settings should consider whether this is the safest and most effective way of sharing images with parents/carers. Settings need to be aware that once images have been shared online, via social media, the setting will be unable to control whether the images are copied, distributed, amended or altered.

Before taking or sharing any photographs or video recordings of children, educational settings need to ensure that they have written consent from their parents or guardians (or permission from the child themselves, if they are over 12 years old and deemed to be competent to make such judgements, as suggested by the Information Commissioner). If you chose to use social media to share images with parents/carers then only setting provided devices, emails or phones should be used and clear boundaries and procedures should be documented within the appropriate policies.

We recommend that school/setting avoid using:

- Personal details or full names (first name and surname) of any child or adult in a photograph.
- Personal contact information such as email, postal addresses, and telephone or fax numbers.

If educational settings use a photograph that could identify and individual child, then they should not include that child's name. If a child is fully named in the text, then it is recommended that settings don't include a photograph of that child. The same advice applies to images of staff and relevant consent should be obtained before sharing their images on official social media channels. This will help reduce the risk of members of the community being identified.

The Kent County Council Image Use Policy contains further information regarding taking images and template consent forms: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

How can leaders, managers, Headteachers and Designated Safeguarding Leads enforce the Social Media policy with parents/carers?

Most educational settings have a contract (or home-school agreement) with parents, to ensure that children and young people's learning and welfare are fully supported both inside and out of the classroom; these include statements for parents, confirming that they will reinforce the settings policies on homework, behaviour and conduct.

In order to counter issues regarding the negative use of social media, a number of educational settings have decided to include a statement on the Home-School Agreement, in an attempt to prevent parents from making derogatory or malicious comments online.

Whilst statements like this may be difficult to manage or enforce, (because they involve parents' personal use of social networking sites), it does show that the educational settings takes this matter seriously and, by signing the agreement, parents accept that they have a responsibility to act appropriately.

Example statements could include:

"We will support the school's approach to online safety and will not upload, share or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community".

OR

"Parents and carers are reminded to use existing structures when making any complaint about the school or a member of staff. They are advised not to discuss any matters on social networking sites'.

OR

'If at any time during your child's time at xxxx school, you wish to make a complaint, then you are advised to follow the school's complaints procedure which can be found on the

school website [insert link]. We recommend that all parents and carers refrain from using social networking sites to discuss sensitive issues about the school.'

Additional content to help engage parents/carers in the official use of social media can be found in annex D and E.

In some cases where educational settings are unwilling or unable to develop an official social media presence, they may find that one develops organically within the wider community. A common instance is when Friends Associations or Parent Teacher Associations or indeed interested parents set up Facebook pages/groups or Twitter accounts to publicise fundraising events or simply to communicate with other parents. It is important that even unofficial groups are run in accordance with the settings policies otherwise they can undermine the wider safeguarding ethos and culture.

It is recommended that leaders work alongside any parents/carers involved in running such groups and provide clear boundaries about appropriate online behaviour. A template disclaimer to support this discussion can be found in annex G. Additionally a template Acceptable Use Policy for parent run social media channels can be found within the Kent County Council Acceptable Use Policy guidance: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

How can leaders, managers, Headteachers and Designated Safeguarding Leads enforce the Social Media policy with learners?

Social media is an everyday form of communication for many children and young people, and forms a vital part of growing up in today's modern society.

'Keeping children safe in education' 2016 (Department for Education) has highlighted that governing bodies and proprietors need to '…*ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum ….*' Educational settings need to ensure that there is a whole school, progressive curriculum which enables children to become safe and responsible users of social media. Children should be given age and ability appropriate opportunities to develop safe online behaviours and should seek to ensure that children are able to identify and manage risks when using social media, both on site and at home.

Whilst many educational settings will choose to block access to social media sites for children, it cannot be assumed that they will not access them offsite, or by using personal devices. Children and young people must therefore be given age appropriate education regarding safe and responsible use of social media, in order to develop the skills and build resilience to manage online issues themselves.

For some educational settings, the benefits of allowing access to social media tools in the classroom, such as teaching learners to apply privacy settings or enabling them to access high quality learning material will outweigh the possible risks. If educational settings choose

to use social media channels within the classroom then annex A, B and C may be helpful to enable leaders to document their decision making.

Some educational settings are choosing to use social media as a communication tool to engage with young people. In these cases, leadership and management should be aware that many popular social media services such as Facebook, Instagram, Twitter and YouTube have age restrictions of 13+, therefore these tools should only be used with learners who meet their requirements.

Educational settings who use social media to communicate directly with learners must be aware of the increased risks. Learners may not always use privacy settings correctly, they may accept friends/follow requests from unknown people or share too much personal information online; this, combined with being clearly identified as members of your school/setting community, could put children at risk of harm both on and offline. Educational settings should consider if and how these risks can be reduced and managed; for example, colleges and sixth form providers may decide that the benefits of social media use with young people outweighs the risks and as such will implement a comprehensive curriculum to educate young people about how to use specific privacy settings etc. before engaging with official social media channels.

The Kent County Council Online Safety policy template and Acceptable Use Policy Template contains further information regarding pupils and social media: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

What should I do if I am concerned about current practice in my education setting?

If educational settings are unsure of their legal responsibilities in relation to the use of social media, they can consult with the relevant person or department from the Local Authority.

Any evidence of inappropriate use of social media by any member of the school/setting community should be reported to the school's/setting's designated safeguarding lead (DSL) who may then consult with Kent County Council (the Education Safeguards Team or LADO), Social Services or the police, if appropriate.