Using Social Media in Educational Settings

Guidance and template resources for Educational Setting Leaders

February 2017

Kent County Council
kent.gov.uk

This document is available in a range of formats and can be explained in other languages. To ask for an alternative version, please email alternativeformats@kent.gov.uk

Kent County Council Equality and Diversity Team, phone with Type Talk: 18001 03000 421553

Or write to: *Kent County Council, Diversity & Equality Team Room G37, Sessions House, County Hall, Maidstone, Kent, ME14 1XQ*

Contents

Core Guidance for Educational Settings

Annex Resources

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

Introduction: Using Social Media in Educational Settings

Social media tools including social networks (such as Facebook and Twitter), video sharing sites, blogs, forums and wikis have become everyday forms of communication for both adults and children; whether accessed through a computer, tablet or smart phone, they help us stay in touch with friends and family, share photos, play games, find out news and information and even help organise events and campaigns.

Social networking and media sites can also have risks; they have changed how we communicate and the boundaries between the "real" world and the "virtual" can become blurred. This can have potentially serious consequences for staff, parents/carers and children who may not be aware of the risks behind every day online activity; people may post unsafe or inappropriate information about themselves and their personal lives online, as well as providing opportunities for offenders to groom and abuse children.

Online social media tools can also be excellent devices learning; providing exciting and new opportunities for educational settings to engage, communicate and collaborate with learners and the wider community. The positive use of social media and Information and Communication Technology (ICT) within educational 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 community are kept safe.

This document has been developed to help educational settings make informed and appropriate choices about using social media tools either within the classroom or as official communication channels. It includes considerations about safe practice in order to protect staff, learners and the wider community. Additional information can be found with the annexes with template resources and additional guidance regarding some of the more popular social media channels.

This guidance is suitable for educational settings including (but not limited to) schools, early year's settings, Pupil Referral Units, 14-19 settings, further education colleges, alternative curriculum provisions, Children Centre's and hospital schools etc. In some cases we have used the terms 'school' and 'pupil' within this document, but stress that its use within other educational settings and beyond are relevant and appropriate but may require adaptation to meet the needs of specific communities, ages and abilities.

Please note this guidance does not seek to replace legal advice regarding educational settings statutory and common law obligations to risk assess as per Health and Safety Law. Leaders may wish to take appropriate legal advice when making these decisions.

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.

Considering the risks posed by Social Media

Please note educational settings have statutory and common law obligations to undertake risk assessments as per Health and Safety Law. This guidance does not seek to replace legal advice, which educational setting leaders may wish to take when making these decisions.

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

Risk assessments should be carried out prior to using any tool or technology in the classroom; it is also good practice to risk assess social networking tools before using them for any official or educational purpose.

When carrying out a risk assessment approach it is recommended that:

- The assessment is carried out by leadership with support from technical and curriculum focused members of staff.
- The policies published (e.g. terms and conditions, privacy, data protection) by any service/website/apps being used should be fully evaluated by the school for privacy and data security (e.g. minimum age)
- The website/app/service's user interface should be tested by an appropriate member of staff (e.g. how to delete and block accounts and moderate content)
- It is important for schools to understand what personal data is collected by the site, 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 material or additional content should also be assessed.

This guidance contains some sample risk assessment templates are provided within this document for schools/settings to use and adapt, however other tools or approaches may be preferred.

When considered cloud based systems (such as Google Apps for Education etc.), schools should access the DfE guidance available here: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

It might also be helpful, in some cases, for Headteachers, managers or leaders to carry at a Privacy Impact Assessment (PIA); a process which enables an organisation to systematically and thoroughly analyse how a project or system will affect the privacy of the individuals involved. An effective PIA will be used throughout the development and implementation of the social media tool. The ICO website has a Code of Practice on PIAs: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Checklist for using Social Media Tools in Educational Settings

Before using any Social Media tool, educational settings might like to consider the following questions:

☑ Does the educational setting need to seek legal advice following any decisions?
- Are you aware of and following the statutory and common law obligations to risk assess, as per Health and Safety Law?

☑ What are the objectives/outcomes for this project?
- What do you want to communicate?
- Who is the intended audience (if using a communication tool)?
- What is the most suitable medium/site to use for this purpose and why?
- Will the project be child, parent/carer or staff led?

☑ 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 approach/ technology over traditional methods of communication or learning?

☑ What is the most suitable medium/site to use for this purpose and why?
- Are there other alternatives?

☑ 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?

☑ Is the Leadership Team actively involved in and aware of the use of Social Media?
- Do you have documented approval and consent from educational setting leaders?

☑ 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)?

☑ How will the site/tool be used?
- Do you have appropriate permissions or consent for any images, documents etc. to be shared?
- 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)?

- ☑ Are you aware of potential privacy issues and restrictions?
  - ▪ Have you explored the sites privacy and control settings?
    - • Do you know the best option for your needs and requirements (e.g. groups vs pages vs profiles)
  - ▪ Can you restrict access to only your intended audience for all or part of the site (this is essential if sharing information you wouldn't share publicly)?
    - • If not, how will you safeguarding your community?
  - ▪ Does the tool offer moderation?
    - • If so, who will be responsible for moderation on a regular basis?
  - ▪ Does the tool/device offer user tracking (if appropriate) to ensure adherence to Acceptable Use Policies?
  - ▪ Do you have appropriate permissions or consent for any images, documents etc. to be shared?

- ☑ Can you support this idea safely and responsibly?
  - ▪ Do you have the resources (people, time etc.) to support this activity?
  - ▪ Does the tool offer moderation?
    - o If so, who will be responsible for moderation on a regular basis?
  - ▪ Do you have a clear strategy in place to respond to negative comments or concerns?
  - ▪ Have you created or adapted your Acceptable Use Policy to reflect your use?
    - o Has this been signed and created for all those involved (this is essential if using a communication tool)?
  - ▪ Does the setting have clear rules/boundaries about safe and appropriate online behaviour?
    - o Have these been communicated to all those involved?
    - o Have all members of the community received up-to-date training regarding safe and responsible online behaviour?

- ☑ Is use of social media covered in the educational setting policies?
  - ▪ Have the appropriate policies been updated to include this use?
  - ▪ How have the policies been communicated to all members of the community?
  - ▪ Has the Online Safety Policy been updated recently?
  - ▪ Has this been communicated to all members of the community?

- ☑ How will you know the project has achieved its aims?
  - ▪ What will "success" look like?
  - ▪ Are you preparing a pilot project first?

Using Social Media as a Professional – Advice for Education Staff

This guidance is intended for educational setting staff who are looking to use social media to officially engage with their communities or are using social media for their own Continuing Professional Development (CPD).

Social networking accounts can offer new ways for education staff to engage with a variety of audiences and allows professionals to engage and debate; ask and answer questions; share knowledge and ideas; create a positive digital footprint and access virtual support networks.

Social networking sites can be a fantastic communication tool for education staffs CPD but the boundaries between the "real" world and the "virtual" can easily become blurred and this can have potentially serious consequences for staff if not carefully managed.

Know your schools policy and procedures
- Make sure that you read, understand and follow your schools code of conduct or "Acceptable Use Policy".
  - Be aware most educational settings state that staff should not add parents or learners (past or present) as friends on any personal social media accounts.
  - Any exceptions (such as pre-existing relationships) or official channels should be discussed with your line manager and/or your settings Designated Safeguarding Lead (DSL).
  - Be aware that you should only use work provided equipment to take and share any images of learners and you must comply with your settings image use policy with regards to have written consent.

- Always ensure that your online behaviour is in line with your employer's policies, legislation and professional guidance. This will include being aware of confidentially, online safety, social media, child protection, data protection, copyright and the Teachers' Standards (as appropriate).

Protect your online reputation
- Your professional reputation is crucial to your current and future career and managing your online reputation is now an essential part of being an education professional.
  - Even if you don't use social networking as a professional tool it's important to be aware of what is online about you so always apply security and privacy settings appropriately. Searching your name regularly on search engines can be a useful way to monitor your online content or 'digital footprint'.

- When using social networking as a professional, it is strongly recommended that you use separate accounts, pages or profiles (essential if communicating with children or the wider school community) for your CPD and personal life. This will help you to ensure that your professional role is clearly separated from your personal.
  - This doesn't mean that you can't show your "human" side online but you should always be mindful to ensure that your online behaviour is compatible with your role and that you can maintain your professional boundaries and relationships.

- Always ask yourself; "would I say or do this in the 'real' world" and "would it be appropriate for a child, their parent/carer or my Headteacher/manager to see this?" before posting any comments, pictures etc. online. If the answer to these questions is no, then it's probably best not to share it online in the first place!

- Posting derogatory comments is never acceptable. Educational staff are required to maintain reasonable standards in their own behaviour, and to uphold public trust in their profession.
  - Civil, legal or disciplinary action could be taken against you if you are found to have posted something online which could bring the profession or institution into disrepute, or if something is felt to have undermined confidence in your professional abilities.
  - It is always important to role model positive behaviour online and be professional online.

- Always be aware that any content posted online can be copied, shared or misinterpreted and can potentially become public and permanent. Content posted online by or about you makes up your digital reputation (this may include content shared by others as well as by yourself) and this can influence perceptions about you, professionally and personally both positively and negatively.

- Be careful not to share any personal contact details or other personal information online, especially with children or their parents/carers. Be aware that many sites or apps share your exact location when you post a comment or pictures from a mobile device or tablet. Information about where you live or work should only be shared with trusted friends and family members.

- Make sure you use a strong password for your online accounts and always logout of accounts and profiles after use.

Safeguarding is essential

- Do discuss your use of social networking, including your understanding of boundaries and safe practice, with your line manager so that your online conduct is open and transparent so as to safeguard yourself and others.

- If you're not sure what you can and can't do online or are unclear about what your policies and procedures permit or require then speak to a member of management, the Designated Safeguarding Lead or your line manager.

- If you see or experience anything online that makes you feel worried, uncomfortable or concerned then always speak to your line manager and/or your settings designated safeguarding lead (DSL) as soon as possible.

Have a clear purpose

- Decide exactly why you want to use a social networking tool – is it for your own professional development or will it used for your setting/department?
  - If you are using social media on behalf of your school then ensure that your leadership team have approved the use. Leaders should risk assessed the use and document the decision (as well as expectations for you to follow) within their social media and acceptable use policies.

- All communication with parents and children must be transparent and open to scrutiny so if you want to use social networking for official communication with pupils and/or parents then it is essential that the leadership team are aware and have fully approved and risk assessed the activity before it takes place.

Reflect and build your networks

- Spend some time learning to use social networking sites safely and effectively. Different sites will have different benefits and risks depending on your aims.
  - Some social networking sites have in depth information and advice in their help sections specifically for educators.

- Ensure that you are aware of online etiquette otherwise known as "netiquette" on the sites you use.

- If you attend CPD events and conferences then use your social media presence to engage in the discussions and share ideas and resources.

- Use your account or profile biography or descriptions etc. to highlight any particular educational interests or experiences to help build online networks and connections.

- Social networking sometimes takes time to build up relevant links and networks so keep engaging by getting involved in some of the many online educational communities such as UK Ed Chat, the Guardians Teacher Network and Kent-Teach.

Social networking can provide education professionals with exciting new opportunities to be creative and innovative both personally and professionally and it's important that staff consider how they will ensure that they have taken all reasonable safeguarding precautions prior to use so that they can protect themselves and others.

Further Advice and Guidance for Educational Settings

- Kent schools and settings can consult with the Education Safeguarding Adviser (Online Protection) or e-Safety Development Officer within the Education Safeguarding Team to discuss ideas and options before using social media tools or technology
    - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety
    - esafetyofficer@kent.gov.uk or 03000 415797

- "Safer Professional Practice with 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 http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety or www.kscb.org.uk

- Childnet has a range of guidance documents regarding cyberbullying and advice for staff regarding protecting themselves:
    - www.childnet.com/teachers-and-professionals/for-you-as-a-professional
    - www.childnet.com/resources/cyberbullying-guidance-for-schools

- The UK Safer Internet Centre has a range of tools are resources:
    - Professional reputation: www.saferinternet.org.uk/advice-centre/teachers-and-professionals/professional-reputation

    - Professional Online Safety Helpline: www.saferinternet.org.uk/professionals-online-safety-helpline

- 360 Degree Safe tool is an online audit tool for schools from the South West Grid for Learning to help schools review current online safety practice: www.360safe.org.uk

Annex A: Risk Assessment Form for the Use of Web Tools and Technology in the Classroom

Notes for use
- A risk assessment should be carried out by both a technical and an educational member of staff and agreed by a member of the school senior leadership team (including the schools child protection coordinator).
- An evaluation of privacy and data security must include an evaluation of the policies for a service (e.g. minimum age) and test procedures for interacting with the service provider, e.g. account deletion. It is important for settings to understand what personal data is collected, how it is used and whether there is an audit trail that tracks back to a real identity.
- Content suitability should be based on an assessment of the impact of introducing a high bandwidth service on to a network and age related categorisation of advertising, images and textual content found on the site.
- These suggestions are not exhaustive and will need to be adapted according to the site and setting

Name of Member of Staff (s):	
Date:	
Site/Service: URL & name	
Description of Service/site:	
Educational Purpose:	Curriculum requirements/justification, aims and objectives.
Other Details:	e.g. • Required for/by specific subjects or syllabus. • Who it is required to be unblocked for e.g. staff/student groups (all students, small groups). • Time limits (e.g. one off lesson, term/scheme of work). • Classroom management approaches (e.g. supervision and education of users)

Summary of Risk Assessment Decision (amend as appropriate)

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
Approval by:	(Name and role) **NB must be leadership**						

Key Issues Identified and Action Required

Risk Identified	Action Taken	Action by	Date

Annex B: Checklist for the Use of Web Tools and Technology in the Classroom

Carried out by member of Leadership Staff:
Additional input was obtained from:
Member of Technical Staff:
Member of Safeguarding Staff:

Date review carried out:
Date to be reviewed (annual recommendation):

Key:

	High risk identified: Unsuitable to use
	Risk Identified: Appropriate action is required/Proceed with caution
	Limited risk

	Yes	No	Further information/discussion
General Considerations			
Endorsed by recognised authority for education use			
Service has good reputation for dealing with concerns (if appropriate)			
Leadership Team Approval			
Use of site is documented in School policies and procedure (if appropriate)			
Appropriate Acceptable Use Policy in place (generic and/or specific)			
Up-to-date whole School Online Safety training is embedded and in place?			
Parental consent required and provided (if appropriate)		If required and not given	
Can/will users be tracked/identified?			
Can/will mobile device management software be installed/used? (if appropriate)			

Privacy and Data Security (for sites/devices that allow students/staff to interact with each other or others)			
Registration of users required?	🟩	🟧	
Anonymous registration possible?	🟧	🟩	
Service can be administered or managed by staff e.g. staff can verify users	🟩	🟧	
Minimum age is suitable for the setting? NB check sites terms & conditions and terms of service.	🟩	🟥	
Privacy tools	🟩	🟧	
Privacy and Data Security			
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 or themes (images, text, videos) NB not educational material relating to appropriate educational subjects such as sex & relationships education	🟥	🟩	

User generated content e.g. photos, videos etc. (be aware content may therefore be unsuitable)			
Advertising Material NB - Be aware of COPPA requirements			
Dating/Personal sites			
Weapons			
Promotion of drugs, alcohol, tobacco etc. (not educational sites)			
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 (if appropriate)			
Moderated by member of staff (if so how often)			
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			
Other (add additional lines as appropriate**)**			

Annex C: Consideration Form for the Use of Social Media

Site considered: _____   **Date:** _____

Member of Staff: _____ **Role:** _____

What are the reasons for using Social Network Site?

What should you do? (As appropriate to your audience)

Consider alternatives e.g. on private/secure networks (e.g. VLE, school website)	❑
Discuss intentions with Leadership team/Line Manager	❑
Survey your intended audience(s)	❑
Inform Parents/Carers of the use of the site	❑
Brief staff to raise awareness about online safety (both personal and the community)	❑
Brief learners to raise awareness and understanding around information sharing on social media	❑
Update policies e.g. social media, image consent, etc.	❑
Agree and display acceptable use policies for use of site (including specific AUPS for admins and users)	❑
Posters/Instructions are shared to help inform users of the agreed rules	❑

Potential Hazard (Please note this list is not exhaustive)	Action to be taken to reduce risks	Ensure that pupils/parents/staff know…..
Online bullying of/by • Learners • Staff • Parents		...what to do if they feel they are being bullied or see bullying online …the schools anti-bullying policy and sanctions
Contact by unknown people • Some social networks can search for people by age and gender so easy for people to be targeted • Members of the community can be clearly identified by unknown and unverified users	..	… how to refuse contact with unknown people ...how to use privacy settings effectively e.g. using "friends" list and checking how posts/content can be viewed ...how to report suspicious contacts
Personal information being made public accidentally or deliberately • Many sites share information publically by default unless you adjust privacy settings • Information made public all around the world instantly • Can add a location which could mean people could identify where you are from • Can enter address or phone details so can be contacted directly. • Admin not being aware of image use and confidentiality requirements		...that once sent information could be seen by anyone ...they need to adjust their privacy settings to keep aspects of the site private …the potential risks of adding their location would mean that they could be found by people they do not know ...the potential risks of listing their personal details …the schools policies regarding confidentiality, data protection etc.

Privacy and data protection • Site may share information with third party suppliers who perform functions • Site may disclose information if required to comply with law, regulation or legal request • In the event Social Network is taken over information may be sold or transferred but privacy policy to still apply.	..	…that the company may share the data with other companies ...that even if they delete the information it is still there and a trace will be left that can still be accessed
Inappropriate photos and tagging • Users sharing photos without consent • Other users tagging people in photos		...that any photo or video on the site could be seen by anyone ...that tagging the photo could lead to identification and therefore contact by people they do not know
Age limits • More social networking sites have an age limit of 13. Therefore it will not be appropriate for pupils under 13	..	…they should only use Social Network if they are old enough ..how to inform the Social Network of the age of user if it contravenes rules
Finances • Some sites have functionality that requires payment		..the dangers of paid services
Behaviour of community members • Site might not mediate content or intervene in disputes between users. • Users are allowed to post content, including potentially inflammatory content, provided that they do not violate the Terms of Service and Rules. • What to do if users have problems is not immediately obvious on the site?		..that they must act legally. ..the AUP makes it clear what users should do if they have a problem and that guidance is available by clicking on help ..Terms of Service and where to find these and any support they might require from the site. … their responsibilities and the sanctions that can be imposed if behaviour breaches school policies

Other		

Decision and Justification

Approved by:_____

Member of Leadership Team: _____(Role)

Date: _____

Annex D: Template Letter when considering using Social Media as Engagement Tool

Although aimed at parents, this letter can also be adapted for use with learners (aged 13+) if wishing to increase learner engagement

Dear Parent(s)/Carer(s)

I am writing to you as the school is exploring different options for communication to ensure that we are able to keep in touch and share news with parents/carers through a variety of different formats. The school is considering using a range of communication channels, including social media tools to support this and would like to begin by seeking ideas and opinions from the school community.

At this stage we are only seeking to gather feedback from parents on a range of communication channels and would like parents to indicate any preferences. The decision will be carefully considered and assessed to ensure that all members of the community are safeguarded. Any use of social media will initially take place on a trial basis and will be reviewed regularly and the school will continue to communicate with parents through a variety of approaches.

Please indicate any preferences for communication channels for the school to consider:

Option (Add or amend as appropriate)	Yes I would use this	No I would not use this	Other comments
School website			
Email			
Text Message			
Newsletter			
Official School Blog			
Official Facebook Page			
Official Facebook Group			
Official Twitter Account			
Official YouTube Account			
Other			

Please be aware that the school is currently considering a range of options and may decide not to proceed due to parental preference or safeguarding considers.

The school would welcome comments regarding this possibility from parents/carers and the Designated Safeguarding Lead (NAME) and myself (if different) are available to discuss any help you may need or concerns that you may have.

Yours sincerely

Headteacher/Manager

Annex E: Template Letter for Educational Settings launching an official Social Media Channel

Dear Parent(s)/Carer(s)

I am writing to inform you that following feedback from parents, the school will be soon be launching a (Insert name of selected communication Channel e.g. Facebook Page) to enable us to communicate and engage with (audience e.g. parents/carers, students if 13+, wider community) on a wider scale.

The school xxxx will be used to communicate with parents/carers and share news, information and achievements with our community. We would like to encourage parents to like/follow/subscribe to our page/account (link) to receive updates. This tool will not replace our other existing communication channels (include example such as school website, newsletters, parent mail, text services, learning platform) but will enable us to communicate and share information with (audience) more effectively. Engagement with the (name of service) is entirely optional.

We would like to make sure that we work in partnership with parents and carers to ensure that the school xxxx is used safely and responsibly to benefit all members of the school community. With internet use becoming an essential feature of everyday life it is important that all members of the school community are aware that online conduct can have a significant impact both within and outside of school. Safeguarding is always our primary concern and our policy guidelines around the acceptable use of images are very clear. We will always seek parental consent before posting images of children. Therefore it is essential we work in partnership together so that all members of the school community are safe on and offline.

In order to do this the school will (list safety approaches e.g. not post any photos of children without written parental consent, monitor the page on a regular/daily basis, block offensive language, deliver staff training.) However we will also need support from parents/carers to ensure that all members of the community are kept safe.

We would like to remind all members of the school community that xxxx is a public domain and we all need to be careful to ensure that the content we post online is safe and appropriate to share. We would like to request that any parents/carers who use the school xxxx post comments with consideration towards others and we request that all comments are polite and respectful and in line with our policies Schools may wish to attach a copy of their Acceptable Use Policy and/or Home School Agreement

The school reserves the right to remove any posts which are abusive or offensive and any comments which may be considered criminal or that cause distress will be removed, reported and managed in

accordance with the school policy (list). The school will not allow solicitations or advertisements from outside companies or groups and are not responsible for any external content linked from this page.

Facebook Page Specific: Remove if the Facebook Page will not allow comments
It is important to point out that should a parent comment, tag themselves (or someone else) on a post or image shared on the schools Facebook page then this will identify parents and potentially their children as being members of our community. Parents are advised to ensure that have appropriate privacy settings in place to safeguarding themselves and their families.

Facebook Group Specific: Remove if the Facebook Group will be Secret
It is important to point out that should a parent join the school Facebook group then this will identify parents and potentially their children as being members of our community. Parents are advised to ensure that have appropriate privacy settings in place to safeguarding themselves and their families.

Twitter Account Specific:
It is important to point out that should a parent follow the school Twitter account then this will identify parents and potentially their children as being members of our community. Parents are advised to ensure that have appropriate privacy settings in place and to carefully consider the content they tweet in order to safeguard themselves and their families.

The school would encourage all (name of service) users to access the appropriate help section for guidance regarding privacy and safety settings and terms of use: Insert link to help pages

You can also find out more about keeping yourself and your children safer online through some of the following links:

- www.thinkuknow.co.uk – Visit the "Parent/Carer" Section and use the "Click CEOP" button to seek advice and report online abuse
- www.childnet.com – Visit the 'Know It All' Section for an interactive guide about online safety
- ww.getsafeonline.org – Free up-to-date Security advice including using complex passwords and managing hacked accounts
- www.saferinternet.org.uk – Information from the UK Safer Internet Centre, including filtering and parental control information
- www.nspcc.org.uk/onlinesafety - Support and advice for parents from NSPCC
- www.internetmatters.org – Information for parents/carers from the four largest Internet Service Providers (BT, Talk Talk, Virgin and Sky).

The Designated Safeguarding Lead (NAME) and myself (if different) are available to discuss any help you may need or concerns that you may have.

Yours sincerely

Headteacher/Manager

Annex F: Template Disclaimer for Educational Settings Official Page/Account

This is a Facebook Page/ Facebook Group/Twitter account/YouTube account for parents/carers of xxxx school community.

We would like to remind all members of our school community that Facebook/Twitter/YouTube is a public domain and we all need to be careful to ensure that the content we post online is safe and appropriate to share.

This site will be monitored by an official member of xxx school staff in accordance with school policy (list). Schools may wish to list other safety approaches.

Xxxx school would encourage all Facebook/Twitter/YouTube users to access Facebook/Twitter/YouTube help section for guidance regarding privacy and safety settings and terms of use: links as appropriate

Schools may wish to share tips and links to resources such as Think U Know, Childnet, Safer Internet Centre etc.

Members of xxx school community are encouraged to read the relevant school policies (e.g. Social Media, Acceptable Use, e-Safety, Child Protection, Complaints, and Image Use etc) and act as role models online. We request that all comments are posted with consideration towards others and are polite and respectful.

xxxx school reserves the right to remove any posts which are abusive or offensive and any comments which may be considered criminal or that cause distress will be removed, reported and managed in accordance with the school policy (list) and the law.

xxxx school will not allow solicitations or advertisements from outside companies or groups and are not responsible for any external content linked from this page.

If any member of the community has any complaints or concerns then they should contact the school directly (list contact information e.g. link to school website)

Annex G: Template Disclaimer for Parent/PTA run Social Media Channel

Also see the Kent Acceptable Use Policy document: http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

The xxxx Parents account/page/group is created and maintained by parents of pupils at xxxx school for the purpose of communicating with other parents whose children currently attend xxxx School. It is not run by the school and as such may not be viewed as an official school communication channel.

All posting of comments on this page/group are at the discretion of the page/group administrators who are volunteer parents within the school community. The intent of this is not to keep any negative or critical information from being posted, but to protect the privacy and rights of xxxx staff, parents and pupils. Naming specific employees, parents or pupils in a negative way will not be allowed. The page/group administrators will review all postings to make sure they do not run afoul of these rules, nor the schools policies, including but not limited to behaviour, child protection, confidentiality, anti-bullying, online safety (social media), use of images and information governance.

We welcome your involvement with the communication channel and look forward to engaging with you. However, we will not allow postings that:

- Contravene any school policies
- Break the law or encourage others to do so. This includes respecting copyright and fair use laws.
- Contain abusive or inappropriate language or statements. This includes remarks that are hateful as well as those that contain obscenities or are sexually explicit.
- Easily identify pupils, parents and/or staff in defamatory, abusive, or generally negative terms.
- Do not show proper consideration for others' privacy or are considered likely to offend or provoke others – i.e. goad others into inflammatory debates.
- Are spam – i.e. repeatedly posting the same comment or comments that are simply advertising/promoting a service or product. If you wouldn't want to receive it yourself, don't post it.
- Are political in nature.

The account/page/group administrators reserve the right to not post or to remove any comments at any time, for any reason, but we hope that will not ever be necessary. We also reserve the right to block individuals who misuse our account/page/group.

If you have a comment or would like to report an inappropriate comment for us to review, send an email to <email address> or contact the Headteacher directly.

Please note the school has its own communication channels (list) and an official website. (If appropriate)

Annex H: What to Consider when Setting Up an Official Facebook Page

Please note this guidance is not exhaustive and is intended to support educational settings in making informed decisions.

Facebook Pages can be created for businesses, brands, organizations and public figures to share their stories and connect with people. 'Pages' can be customized with stories, events and more. People who like a 'page' will then get updates in their 'News Feed'.

More information about setting up a Facebook page can be found here: https://www.facebook.com/help

Why would a school/setting want a Facebook page?

- A Facebook page can be a useful and free way of publicising your school/setting and promoting activities and useful information
- Facebook pages can be quick and easy to set up and can have significant benefits for learning, communication, engagement and participation.
- It enables you to go to where your parents are: many parents rarely check your official website, but may engage with their Facebook account daily – it's a good way of linking to information you want them to be aware of.
- Many schools and settings have found that Facebook pages have already been automatically created either by well-meaning parents or staff or due to people tagging themselves via geo-location services in status updates or photos. By creating an official page or claiming an existing one then the school/setting will have more control over its digital reputation.
- Advertising - prospective parents may search for your school/setting within Facebook and you will want the top search result to be the 'official' page!
- It is important to note that information on a Facebook page should also be available elsewhere online e.g. school/setting website, Twitter, learning platform, newsletter etc.

What can a Facebook Page offer your school/setting?

- Sharing
  - Sharing links to your website or learning platform.
  - Sharing links to information for parents.
  - Sharing information about what's happening at your school/setting.
- Consultation
  - Schools and settings can use Facebook pages for gathering information e.g. by using polls. They are simple to set up and can give you quick data on key issues
    .

- Creating an official web presence
    - The school/setting can take ownership of its online identity and maintain an official online presence which is easier to manage than unofficial pages or content.
    - Linking with existing social networks e.g. official Twitter feeds can make it easier to manage a Facebook page – content can be published from the Twitter feed directly to the Facebook page.

What are some of the risks of having an official Facebook Page?

- Facebook Pages are always public and schools/settings cannot limit who can like and access the content shared.
    - All content posted must therefore always be appropriate for a worldwide audience and have appropriate parental consent etc.
- People could post inappropriate comments or pictures for example spam selling/promoting products or threats to members of the community.
- Unknown people could "Like" the page. The setting cannot prevent this but can regularly check and block/report any accounts which concern them.
- Children, parents or staff could be identified as members of the school/settings and could be placed at risk of harm or harassment.
- Underage children (12 or under) could "like" the page.
- The page could be hacked and manipulated.
- Admins could post content which breaches confidentiality or places children or other members of the community at risk.
- The page could be used to complain about the school/setting or to harass members of the community.

What do you need to consider before setting up a Facebook page?

- Be clear about your aims and objectives – know why you want to set up a Facebook Page and how it will benefit your school/setting.
    - How will you know if this has been achieved? For example it will be classed as successful if 25% of parents will "like" the page.
- Start with consulting with your own community.
    - Consider if there is demand for Facebook. For example if parents do not want a Facebook page then there is little point in setting it up!
    - Consider what other options are available and how it can complement existing communication channels.
    - Be aware that using a Facebook account rather than a group or page to promote a "business" is against Facebook's terms and conditions and schools/settings could risk having accounts closed without notice. Using accounts which "friend" parent or children rather than an official page can also increase the risk of allegations and safeguarding concerns. Therefore the official use of pages and groups is recommended.
- Complete a risk assessment to identity possible hazards and what action can be undertaken to reduce possible concerns.

- Ensure that leaders and managers are engaged with the page and that all members of staff are following appropriate policies e.g. the Acceptable Use, e-Safety and data protection policy
- Consider trialling the page with a class or a year group before whole-school/setting rollout e.g. 'XXXX School Year 6 Parents page'. This will help bring out any issues around content, privacy or settings.

Who should be the Administrators of an official Facebook page?

- It is advisable that the admin is a member of the leadership or management team.
- It is advisable to have more than one admin, as content should be updated regularly and sufficient time will need to be allocated to allow this.
  - o Schools/settings will need to consider how this can be managed.
- An administrator needs to have a separate professional Facebook account (rather than a personal one) and the school/setting page will be linked from this. Check that the other admins have also set up a professional Facebook account to protect against risk and reduce vulnerability for staff.
- The school/setting will need to ensure that all admins have signed an appropriate Acceptable Use Policy and have accessed sufficient training to enable them to manage the page successfully. Admins must be professional at all times and be aware that they are an ambassador for the school/setting.
- Consider how admins will access the page e.g. via a school/setting provided device.
  - o It won't be appropriate for members of staff to use their personal devices if they are uploading photos of children so they school/setting will need to provide appropriate resources and access.
- Ensure the admins use a strong password which is only available to the admin and the leadership or management team in order to reduce the risk of the site being hacked.

Who should we allow to post onto the official Facebook page?

- When setting up the page you will have options to set permissions on your page – who can post and who can comment.
  - o Schools and Settings might wish to consider removing the option for people to comment or post as this may lead to inappropriate responses.
  - o It's a good idea to start off by limiting these permissions initially. If a school/setting ultimately decides it would like to expand the permissions it offers its followers, it's easy to do so. **It's better to become more permissive than more restrictive.**
  - o Schools and settings can create and manage lists of blocked words and terms. Schools/settings may wish to add names of staff or local terms/slang which they would prefer not to have posted on the page.
- Be aware that limiting posting ability won't prevent Facebook followers from liking the page or posts.
- Facebook are known for often changing the way privacy and security settings are displayed or administered.

- o Be prepared to change your settings if Facebook make overall changes – subscribe to the Facebook Safety page to keep updated on any changes.

Can we involve children aged 12 or under in using an official Facebook page?

- Facebook's age limit is for children aged 13 and over, so it is inappropriate to use an official Facebook group to directly communicate or inform children under 13.
- When engaging with children aged 13+ then schools/settings will need to appropriately assess the decision, considering benefits and risks. Schools/settings will need to demonstrate that all reasonable precautions have been taken to reduce the risks of children being identified.
- Schools/settings will also need to ensure that information can be accessed in other ways e.g. Twitter, school website or learning platform for those not wishing to engage with Facebook.

Can we share photographs and videos on the official Facebook page?

- Photos and videos of school/setting activity can be a good way of sharing events with parents.
- Schools should ensure that the correct settings are used to prevent followers from tagging people in the photos.
  - o Schools/settings should also consider storing the photos in a more secure location e.g. the official website or learning platform, and then linking to them from the Facebook page.
- Admins must ensure that they adhere to your policy on publishing children's photos e.g. no names of children published and ensure children are appropriately clothed.
- Schools and settings should ensure that image consent forms are up-to-date and cover the use of social media

What should we avoid posting on an official Facebook Page?

- Admins should consider not mentioning specific details when discussing trips and events etc., as there might be child protection issues around revealing where children or staff are going and when, on a public site.
- Admins must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Leaders must ensure there is a clear procedure for admins to follow if there is a concern, for example reporting to the Designated Safeguarding Lead.
  - o Admins should not engage in public debates if opinions or concerns are raised.
  - o Admins should be cautious when deleting comments, unless they contain credible threats or offensive comments. Opportunities to engage with parents/carers and demonstrate that the school/setting listens to the community might be missed if legitimate comments are removed.
- Admins must not engage with any private messaging with children or parents/carers.

How do I claim an unmanaged Page that exists for my School?

A Page may exist for your schools even if you or someone from your school didn't create it. This can happen for a variety of reasons. For example, when someone checks into a place that doesn't already have a Page, an unmanaged Page is created to represent the location.

If a Page is unmanaged, you'll see in the top right of the Page.

To request to claim an unmanaged Page, use an approved (by the school, not a personal account) Facebook account:

- o Click and select "Is this your business"?
- o Follow the on-screen instructions
- o Be aware that you may be asked to provide information to verify your relationship with the school, such an official phone number, email or documents.

You will need to allow up to one week for your request to be reviewed. If your request is accepted, then you'll become an admin of the Page and may also be able to merge the Page with any duplicate Pages (for example official school Pages) that you have.

Note: Unmanaged Pages that represent geographic locations aren't eligible to be claimed and if a Page is managed, then you won't see the option to claim it. You will need to report the Page to Facebook.

How can I merge two pages?

If you're an admin of both Pages, then you may be able to merge them. This option is only available for Pages that represent the same thing and have similar names. If your Pages have physical locations, make sure the addresses are the same.

To merge your Pages:

1. Go to www.facebook.com/pages/merge
2. Select the Page you want to keep from the first dropdown menu, then select the Page you want to merge from the second dropdown menu
3. If your Pages can be merged, click **Confirm**

The people who like your Pages and any check-ins will be combined, but posts, photos, reviews, ratings and the username will be deleted from the Page you merge. The Page you want to keep will remain

unchanged, except for the addition of people who like the Page and check-ins that were merged from the other Page. The Page you don't want to keep will be removed from Facebook, and you won't be able to unmerge it.

Note: If you don't see the option to merge your Pages, it means that your Pages aren't eligible to be merged. If you see the option to request to merge your Pages, your request will be reviewed by Facebook.

How do I report a Page?

If you are concerned that a Page has been set up claiming to represent your school then:

1. Go to the Page you want to report
2. Click •••on the Page's cover photo
3. Select **Report Page**
4. Choose the option that best describes the issue and follow the on-screen instructions

Facebook will review the Page and remove anything that doesn't follow the Facebook Community Standards. Facebook may also warn or disable the person responsible.

Publishing a Facebook Page

- Once you've created your Facebook page, it doesn't have to be made public until you're ready.
    - Consult management, staff and parents before publishing the page to ensure that it's a good reflection of what's happening in your school/setting.

Evaluating a Facebook Page

- Once your Facebook page is live, ensure you set a timeframe in which to evaluate its success and have clear aims and objectives to help you measure this.
    - If a concern occurs, revisit your training and policies and identify any lessons to be learnt.
    - Involve all members of the community in reviewing the success (or not) of the Facebook Page – have they had a good or bad experience and do they have any constructive comments or views to help inform you?

Annex I: What to Consider when Setting Up an Official Facebook Group

Please note this guidance is not exhaustive and is intended to support educational settings in making informed decisions.

Facebook Groups are a restricted area within Facebook that can be shared with selected 'Friends' or members of the community. A 'group' allows full access to the features of Facebook, but can be restricted, so only users who are 'given access' can see all the information.

More information about managing a Facebook Group can be found at
https://www.facebook.com/help/162866443847527/

Should we have a Facebook Page, Group or account?

- Pages allow schools and settings to communicate broadly with their communities. Pages should only be created and managed by official representatives. Groups provide a space for people to communicate about shared interests. Groups can be created by anyone. Facebook accounts are for personal use.
    - Be aware that using a Facebook account rather than a group or page to promote a "business" is against Facebook's terms and conditions and schools/settings could risk having accounts closed without notice. Using accounts which "friend" parent or children rather than an official page can also increase the risk of allegations and safeguarding concerns. Therefore the official use of pages and groups is recommended.
- Pages
    - **Privacy:** Page information and posts are public and generally available to everyone on Facebook.
    - **Audience:** Anyone can like a Page to connect with it and get News Feed updates. There is no limit to how many people can like a Page.
    - **Communication:** People who help manage a Page can publish posts as the Page. Page posts can appear in the News Feeds of people who like the Page. Page owners can also create customized apps for their Page and check Page Insights to track the Page's growth and activity.
- Groups

    - **Privacy:** In addition to a public setting, more privacy settings are available for groups. In secret and closed groups, posts are only visible to group members
    - **Audience:** You can adjust group privacy to require members to be approved or added by admins. When a group reaches a certain size, some features are limited. The most useful groups tend to be the ones you create with small groups of people you know.

o **Communication:** In groups, members receive notifications by default when any member posts in the group. Group members can participate in chats, upload photos to shared albums, collaborate on group docs and invite members who are friends to group events.

Why would a school/setting want a Facebook Group?

- A Facebook group can be a useful and free way of allowing members of your community to have "private" conversations. This is not something that a Facebook page can offer.
- Facebook groups can be quick and easy to set up and can have significant benefits for learning, communication, engagement and participation.
- Groups enable settings to go where your parents are: many parents rarely check your official website, but may engage with their Facebook account daily – it's a good way of linking to information you want them to be aware of.
- It is important to note that information on a Facebook group should also be available elsewhere online e.g. school/setting website, Twitter, learning platform, newsletter etc.

What are some of the risks of having a Facebook Group?

- Facebook groups must be set up by a Facebook user and will be associated with a profile – school/setting staff may use their own personal accounts to manage groups which could blur professional boundaries.
    - o If members of staff are identifiable and do not have appropriate privacy settings or appropriate understanding of professional boundaries and behaviour then this could put themselves or others at risk.
- To join the group, users must have a Facebook account – this could exclude some members of the community.
- Users may assume that because the group is 'private' that content cannot be shared.
    - o All content posted must always be appropriate for a worldwide audience and have appropriate parental consent etc.
- Members of the group could post inappropriate comments or pictures for example spam selling/promoting products or threats to members of the community.
- If the group is open or closed then children, parents or staff could be identified as members of the school/settings which could place them at risk of harm or harassment.
- Underage children (12 or under) or unknown individuals could try and join the group
- The group could be hacked and manipulated.
- Admins could post content which breaches confidentiality or places children or other members of the community at risk.

Public, Closed or Secret Groups?

When you create a group, you can choose 3 privacy settings: **Public**, **Closed** and **Secret**.
The table below shows who can join these groups and what people can see about them.

	Public	Closed	Secret
Who can join?	Anyone can join or be added or invited by a member	Anyone can ask to join or be added or invited by a member	Anyone, but they have to be added or invited by a member
Who can see the group's name?	Anyone	Anyone	Current and former members
Who can see who's in the group?	Anyone	Anyone	Only current members
Who can see the group description?	Anyone	Anyone	Current and former members
Who can see the group tags?	Anyone	Anyone	Current and former members
Who can see what members post in the group?	Anyone	Only current members	Only current members
Who can find the group in search?	Anyone	Anyone	Current and former members
Who can see stories about the group on Facebook (ex: News Feed and search)?	Anyone	Only current members	Only current members

- Schools and settings will need to consider which option works best for their needs following a risk assessment.
  - It is recommended that school/settings groups are secret to ensure membership lists are hidden from all but other members.

What do schools/settings need to consider when setting up a Facebook group?

- **Before setting up:**
  - Be clear about your aims and objectives – know why you want to set up a Facebook group and how it will benefit your school/setting.
    - How will you know if this has been achieved?
    - What will a Facebook group offer instead of a page?
  - Start with consulting with your own community.
    - Consider if there is demand for a Facebook group. For example if parents do not want a Facebook group then there is little point in setting it up!
    - Consider what other options are available and how it can complement existing communication channels.
  - Complete a risk assessment to identity possible hazards and what action can be undertaken to reduce possible concerns. Consider if the school require an open, closed or secret group. This will depend on the ages and objectives and community targeted.

- Ensure that leaders and managers are engaged with the management of the group and that staff are following appropriate policies e.g. the Acceptable Use, e-Safety and data protection policy
- Consider trialling the group with a group of staff, parents or students or class/year group before whole-school/setting rollout e.g. 'XXXX School Year 6 Parents group or 'History department'. This will help bring out any issues around content, privacy or settings.

Who should be the Administrators of an official Facebook group?

- It is advisable that the admin is a member of the leadership or management team.
  - It is advisable to have more than one admin, as content should be updated regularly and conversations and content may need to be moderated and sufficient time will need to be allocated to allow this. Schools/settings will need to consider how this can be managed.
- An administrator needs to have a separate **professional Facebook account** (rather than a personal one) and the school/setting page will be set up using this.
  - Check that the other admins have also set up a professional Facebook account to protect against risk and reduce vulnerability for staff.
- The school/setting will need to ensure that all admins have signed an appropriate Acceptable Use Policy and have accessed sufficient training to enable them to manage the page successfully. Admins must be professional at all times and be aware that they are an ambassador for the school/setting.
- Consider how admins will access and manage the group e.g. via a school/setting provided device.
- It won't be appropriate for members of staff to use their personal devices if they are uploading photos of children so they school/setting will need to provide appropriate resources and access.
- Ensure the admins use a strong password which is only available to the admin and the leadership or management team in order to reduce the risk of the site being hacked.
- It is advised that groups are set to 'secret' and users are invited to join via email.

Who should we allow to post onto the official Facebook group?

- When setting up the group you will have options to set permissions on your page – who can post and who can comment.
  - Schools and Settings might wish to consider removing the option for people to comment or post as this may lead to inappropriate responses. It can also be set so that admins have to approve posts before they can be viewed.
  - It's a good idea to start off by limiting these permissions initially. If a school/setting ultimately decides it would like to expand the permissions it offers its followers, then it's easy to do so. **It's better to become more permissive than more restrictive.**
- Facebook groups can allow members to add others – it is advisable that schools/settings ensure that new members are approved by an admin (and can be verified as a legitimate member of the community) before they can join.

- Although a Group limits who has initial access to content, users should be advised that there is a need to treat anything posted anywhere on the Internet as public. Users should be advised not to post anything that could be in the least bit contentious or breach any existing policies.
- Facebook are known for often changing the way privacy and security settings are displayed or administered.
  - Be prepared to change your settings if Facebook make overall changes – subscribe to the Facebook Safety page to keep updated on any changes.

Can we involve children aged 12 or under in using an official Facebook group?

- Facebook's age limit is for children aged 13 and over, so it is inappropriate to use an official Facebook group to directly communicate or inform children under 13.
- When engaging with children aged 13+ then schools/settings will need to appropriately assess the decision, considering benefits and risks. Schools/settings will need to demonstrate that all reasonable precautions have been taken to reduce the risks of children being identified.
- Schools/settings will also need to ensure that information can be accessed in other ways e.g. Twitter, school website or learning platform for those not wishing to engage with Facebook.

Can we share photographs and videos on the official Facebook group?

- Photos of school/setting activity can be a good way of sharing events and information with parents, students and staff.
- Schools/settings should also consider storing the photos in a more secure location e.g. the official website or learning platform, and then linking to them from the Facebook group.
- Admins must ensure that they adhere to the school policy on publishing children's photos e.g. no names of children published and ensure children are appropriately clothed.
- Schools and settings should ensure that image consent forms are up-to-date and cover the use of social media

What should we avoid posting on an official Facebook group?

- Admins should consider not mentioning specific details when discussing trips and events etc., as there might be child protection issues around revealing where children or staff are going and when.
- Admins must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Leaders must ensure there is a clear procedure for admins to follow if there is a concern, for example reporting to the Designated Safeguarding Lead.
  - Admins should not engage in public debates if opinions or concerns are raised.
  - Admins should be cautious when deleting comments, unless they contain credible threats or offensive comments. Opportunities to engage with parents/carers and demonstrate that

the school/setting listens to the community might be missed if legitimate comments are removed.
- Admins must not engage with any private messaging with children or parents/carers.

How do I report a group?

If you are concerned that a group has been set up claiming to represent your school then:

1. Go to the group you want to report
2. Click ●●●on the top-right corner
3. Select **Report Group**
4. Choose the option that best describes the issue and follow the on-screen instructions

Facebook will review the group and remove anything that doesn't follow the Facebook Community Standards. Facebook may also warn or disable the person responsible.

Publishing a Facebook group

- Once you've created your Facebook group, members do not have to be invited until the school/setting is ready.
  - o Consult with management, staff and parents before publishing the page to ensure that it's a good reflection of what's happening in your school/setting.

Evaluating a Facebook group

- Once your Facebook group is live, ensure you set a timeframe in which to evaluate its success and have clear aims and objectives to help you measure this.
  - o If a concern occurs, revisit your training and policies and identify any lessons to be learnt.
  - o Involve all members of the community in reviewing the success (or not) of the Facebook group – have they had a good or bad experience and do they have any constructive comments or views to help inform you?

Annex J: What to Consider when Setting Up an Official Twitter Account

Please note this guidance is not exhaustive and is intended to support educational settings in making informed decisions.

Twitter is an information network or micro-blogging site where users can send messages of up-to 140-characters, called 'Tweets'. Users can be "followed" by other users. Users can choose to follow anyone and anyone can choose to follow them unless they restrict access. Once users send a tweet, it immediately appears on their home page, on their followers' pages, and can be searched on Twitter and beyond.

Educational settings can use Twitter to highlight their own news and events but can also follow other local educational settings, local organisations, other educators, famous authors and individuals.

Further information about setting up a Twitter account can be found here:
https://business.twitter.com/en/basics/create-a-twitter-business-profile.html

Twitter's help section also has advice here: https://support.twitter.com/

Why would a school/setting want a Twitter account?

- A Twitter account can be a useful and free way of publicising your school/setting and promoting activities and useful information
- Twitter accounts can be quick and easy to set up and can have significant benefits for learning, communication, engagement and participation.
- Twitter enables you to go to where your parents are: many parents rarely check your official website, but may engage with their Twitter account more frequently – it's a good way of linking to information you want them to be aware of.
- By creating an official Twitter account then your school/setting will have more control over its digital reputation.
- Advertising - prospective parents may search for your school/setting within Twitter and you will want the top search result to be the 'official' account!
- It is important to note that information on a Twitter account should also be available elsewhere online e.g. school/setting website, Facebook, learning platform, newsletter etc.

What can a Twitter account offer your school/setting?

- Sharing
  - o Sharing links to your website or learning platform.
  - o Sharing links to information for parents.
  - o Sharing information about what's happening at your school/setting.

- Consultation
  - Schools and settings can use Twitter accounts for gathering information e.g. by using polls. They are simple to set up and can give you quick data on key issues.
- Creating an official web presence
  - The school/setting can take ownership of its online identity and maintain an official online presence which is easier to manage than unofficial pages or content.
  - Linking with existing social networks e.g. official Facebook pages can make it easier to manage a Twitter – content can be published from the Facebook page directly onto Twitter.
- Engagement
  - Schools and settings can use Twitter accounts to engage with local and national events, such as Safer Internet Day or anti-bullying week.
  - Twitter can be used to build up local networks with other educational settings and local businesses.
  - They can be used to create learning opportunities such as "following" and engaging with popular authors', education figures or other important agencies or individuals.

What are some of the risks of having an official Twitter account?
- By default Twitter accounts are public and the account can be followed and have their tweets shared, viewed and copied by anyone.
  - All content posted must therefore always be appropriate for a worldwide audience and have appropriate parental consent etc.
- Other users could post inappropriate comments or pictures for example spam selling/promoting products or threats to members of the community.
- Children, parents or staff could be identified as members of the school/settings and could be placed at risk of harm or harassment.
- Underage children (12 or under) could "follow" the account.
- The page could be hacked and manipulated.
- Admins could post content which breaches confidentiality or places children or other members of the community at risk.
- The setting could be subjected to tweets which complain about the school/setting or to harass members of the community.

What do you need to consider before setting up a Twitter account?
- Be clear about your aims and objectives – know why you want to set up a Twitter account and how it will benefit your school/setting.
  - How will you know if this has been achieved? For example it will be classed as successful if 25% of parents follow the account?
- Start with consulting with your own community.
  - Consider if there is demand for Twitter. For example if parents do not use Twitter then there is little point in setting it up!

- Consider what other options are available and how it can complement existing communication channels.
- Complete a risk assessment to identity possible hazards and what action can be undertaken to reduce possible concerns.
- Ensure that leaders and managers are engaged with the page and that all members of staff are following appropriate policies e.g. the Acceptable Use, e-Safety and data protection policy
- Consider trialling the account with a class or a year group before whole-school/setting rollout e.g. 'XXXX School Year 6 Parents Twitter account'. This will help bring out any issues around content, privacy or settings.

Who should be the Administrators of an official Twitter account?
- The school/setting will need to set up an official and specific Twitter account
  - Consider if one Twitter account is sufficient – this is likely to be fine for an early years setting or primary school but a college or secondary school may wish to have official accounts for different departments.
- It is advisable that the main admin for the Twitter is a member of the leadership or management team.
  - In some cases it will be appropriate to have more than one admin, as content should be updated regularly and follower's etc. may need to be checked to ensure they are suitable. Sufficient time will need to be allocated to allow this and schools/settings will need to consider how this can be managed.
- The school/setting will need to ensure that any admins have signed an appropriate Acceptable Use Policy and have accessed sufficient training to enable them to manage the Twitter account(s) successfully. Admins must be professional at all times and be aware that they are an ambassador for the school/setting.
- The school/setting will need to consider how admins will access and manage the account e.g. will they have a school/setting provided device.
  - It won't be appropriate for members of staff to use their personal devices if they are uploading photos of children so they school/setting will need to provide appropriate resources and access.
- Ensure the admins use a strong password which is only available to the admin and the leadership or management team in order to reduce the risk of the site being hacked.

What are the privacy options for a Twitter account?
- Twitter accounts are public by default. If Tweets are public then schools/settings need to be aware that everyone (not just twitter users) can see their tweets, anyone can retweet them and anyone can choose to follow them.
- Users can choose to restrict their account which means that Tweets will only be seen by approved followers who have been accepted onto their following list.
  - This gives schools/settings control over who can see their content. Many schools/settings choose this approach initially to begin to understand how Twitter operates etc.

- Some schools/settings only accept followers once they have received additional verification from the user to ensure they are known members of the community, such as an email to the school office with their name and their Twitter name. This reduces risks of unknown people viewing content. It does require administration work and schools/settings will need to regularly review the account to approve or reject request and also to remove users once they are no longer members of the school community.
- Restricted tweets will not appear in any searches. This can be a downside if the educational setting wishes to engage in a wider debate such as sharing pupils learning in relation to national events.

Can we involve children aged 12 or under in using an official Twitter account?

- Twitters age limit is for children aged 13 and over, so it is inappropriate to use an official Twitter account to directly communicate or inform children under 13.
- When engaging with children aged 13+ then schools/settings will need to appropriately assess the decision, considering benefits and risks. Schools/settings will need to demonstrate that all reasonable precautions have been taken to reduce the risks of children being identified.
- Schools/settings will also need to ensure that information can be accessed in other ways e.g. Facebook, school website or learning platform for those not wishing to engage with Twitter.

Can we share photographs and videos on the official Twitter account?

- Photos of school/setting activity can be a good way of sharing events and information with parents, students and staff.
- Schools/settings should also consider storing the photos in a more secure location e.g. the official website or learning platform, and then linking to them from the Twitter account
- Admins must ensure that they adhere to the policy on publishing children's photos e.g. no names of children published and ensure children are appropriately clothed.
- Schools and settings should ensure that image consent forms are up-to-date and cover the use of social media.

What should we avoid posting on an official Twitter account?

- Admins must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Admins should avoid mentioning specific details when discussing trips and events etc., as there might be child protection issues around revealing where children or staff are going to be and when.
- Leaders must ensure there is a clear procedure for admins to follow if there is a concern, for example reporting to the Designated Safeguarding Lead.
  - Admins should not engage in public debates if opinions or concerns are raised.

- o Admins should be cautious when deleting comments, unless they contain credible threats or offensive comments. Opportunities to engage with parents/carers and demonstrate that the school/setting listens to the community might be missed if legitimate comments are removed.
- Admins must not engage with any private messaging with children or parents/carers.

How do I report a Twitter account or Tweet?

- The Twitter Trust & Safety team responds to potential violations of the Twitter Rules: https://support.twitter.com/articles/18311#
- When you report a concern to Twitter you'll need the following information::
  - o A detailed description of your issue
  - o Direct links to any Tweets you'd like Twitter to review
    - To find the direct links to individual Tweets, see the help page: https://support.twitter.com/articles/80586-how-to-link-directly-to-an-individual-tweet)
- Twitter may take action regarding issuing including Brand and Trademark Complaints, Breach of Privacy, Harassment and Violent Threats and Impersonation (unless the account is clearly identified as unofficial or a parody).
- You can find out more information about reporting violations to Twitter here: https://support.twitter.com/categories/284

Evaluating a Twitter account

- Once your Twitter account is live, ensure you set a timeframe in which to evaluate its success and have clear aims and objectives to help you measure this.
  - o If a concern occurs, revisit your training and policies and identify any lessons to be learnt.
  - o Involve all members of the community in reviewing the success (or not) of the Twitter account – have they had a good or bad experience and do they have any constructive comments or views to help inform you?

Useful Twitter Terms to know

- **"@"** - The @ sign is used to call out usernames in Tweets, like this: Hello @Twitter! When a username is preceded by the @ sign, it becomes a link to a Twitter profile.
- **Blocking** - To block someone on Twitter means they will be unable to follow you or add you to their lists, and Twitter will not deliver their mentions to your mentions tab. https://support.twitter.com/articles/117063-how-to-block-users-on-twitter
- **Deactivation** - A way to remove your profile from Twitter. Information from deactivated profiles remains in Twitters system for 30 days. Learn how to deactivate your account here: https://support.twitter.com/articles/15358-how-to-deactivate-your-account
- **Direct Message** – This is also called a DM. These Tweets are private between the sender and recipient (unless a user chooses to share or copy the DM).
- **Email Notifications** - Preferences set by Twitter users to regulate notifications via email about events on your account, such as new followers and new direct messages. Read about how to change your email preferences here: https://support.twitter.com/articles/127860-how-to-change-your-email-preferences#
- **Favourite** - To favourite a Tweet means to mark it as one of your favourite messages. You can favourite a tweet by clicking the yellow star next to the message.
- **Geolocation / Geotagging** - The use of location data in Tweets to tell Twitter and your followers where you are in real time. Is also called "Tweet with Your Location." Learn how to safely Tweet with your location here: https://support.twitter.com/articles/78525-about-the-tweet-location-feature#
- **Hashtag -** The # symbol is used to mark keywords or topics in a Tweet and can be used to find intresting or current topics. Find out more about using Hashtags here: https://support.twitter.com/articles/49309-what-are-hashtags-symbols#
- **Mention** - Mentioning another user in your Tweet by including the @ sign followed directly by their username is called a "mention". This also refers to Tweets in which your username was included.
- **Retweet** - The act of forwarding or sharing another user's Tweet to all of your followers. This is seen as twitter as "RT"
- **Verification** - A process whereby a user's Twitter account is "stamped" to show that a legitimate source is authoring the account's Tweets. Users should be aware that this is not always 100% accurate.

Annex K: What to Consider when setting up an Official YouTube Channel

Please note this guidance is not exhaustive and is intended to support educational settings in making informed decisions.

YouTube is a video sharing service where users can watch, like, share, comment and upload videos globally. Educational settings can use YouTube to upload videos which can then be shared, commented and viewed.

Why would a school/setting want a YouTube channel?

- A YouTube channel can be a useful way of celebrating success or sharing ideas and learning with the wider community – such as helping parents/carers understand specific elements within the curriculum.
- YouTube channels can be quick and easy to set up and can have significant benefits for learning, communication, engagement and participation.
- Advertising - prospective parents may search for your school/setting within YouTube and you will want the top search result to be the 'official' account!
- It is important to note that information on a YouTube channel should also be available elsewhere online e.g. school/setting website, Facebook, Twitter, learning platform, newsletter etc.

What can a YouTube channel offer your school/setting?

- Sharing
  - Celebrating success and learning
  - Communicating with and involving members of the community who may be unable to physically attend events e.g. the school play
  - Sharing information with parents e.g. teaching children about specific activities and techniques

- Creating an official web presence
  - The school/setting can take ownership of its online identity and maintain an official online presence which is easier to manage than unofficial pages or content.
  - Linking with existing social networks e.g. sharing video content onto a school Facebook page.

What are some of the risks of having an official YouTube channel?

- By default YouTube channels are public therefore any content posted on YouTube can be viewed, shared and potentially copied by anyone.

- All content posted must therefore always be appropriate for a worldwide audience and have appropriate parental consent etc.
- By default other users can like or dislike videos or post comments.
  - Other users could post inappropriate comments or pictures for example spam selling/promoting products or threats to members of the community.
- Children, parents or staff could be identified as members of the school/settings and could be placed at risk of harm or harassment.
- Underage children (12 or under) could subscribe to the account.
- The page could be hacked and manipulated.
- Admins could post videos which breach data protection, confidentiality or that could place children or other members of the community at risk.
- The setting could be subjected to comments which complain about the school/setting or harass members of the community.
- Schools/settings could post content such as music scores etc. or images which breach copyright legislation.
- Photos of school/setting activity can be a good way of sharing events and information with parents, students and staff.
- Schools/settings should also consider storing the photos in a more secure location e.g. the official website or learning platform, and then linking to them from the Twitter account

What do you need to consider before setting up a YouTube channel?
- Be clear about your aims and objectives – know why you want to set up a YouTube channel and how it will benefit your school/setting.
  - How will you know if this has been achieved? For example it will be classed as successful if 25% of parents like your content?
- Start with consulting with your own community.
  - Consider if there is demand for a YouTube channel. For example if parents do not watch content on YouTube then there is little point in setting it up!
  - Consider what other options are available and how it can complement existing communication channels.
- Complete a risk assessment to identity possible hazards and what action can be undertaken to reduce possible concerns.
- Ensure that leaders and managers are engaged with the YouTube channel and that all members of staff are following appropriate policies e.g. the Acceptable Use, e-Safety and data protection policy
- Consider trialling the YouTube channel with a class or a year group before whole-school/setting rollout e.g. 'XXXX School Year 6 Parents YouTube channel'. This will help bring out any issues around content, privacy or settings.
- Admins must ensure that they adhere to the policy on publishing images e.g. written parental consent; no names of children published and ensure children are appropriately clothed.
- Schools and settings must ensure that image consent forms are up-to-date and cover the use of social media.

Who should be the Administrators of an official YouTube channel?

- The school/setting will need to set up an official and specific YouTube channel
  - Consider if one YouTube channel is sufficient – this is likely to be fine for an early years setting or primary school but a college or secondary school may wish to have official accounts for different departments.
- It is advisable that the main admin for the YouTube channel is a member of the leadership or management team.
  - In some cases it will be appropriate to have more than one admin and schools/settings will need to consider how this can be managed.
- The school/setting will need to ensure that any admins have signed an appropriate Acceptable Use Policy and have accessed sufficient training to enable them to manage the YouTube channel account(s) successfully. Admins must be professional at all times and be aware that they are an ambassador for the school/setting.
- The school/setting will need to consider how admins will access and manage the account e.g. will they have a school/setting provided device.
  - It won't be appropriate for members of staff to use their personal devices if they are uploading videos of children so the school/setting will need to provide appropriate resources and access.
- Ensure the admins use a strong password which is only available to the admin and the leadership or management team in order to reduce the risk of the site being hacked.

What are the privacy options for a YouTube channel?

- YouTube channels are public by default. If videos are public then schools/settings need to be aware that everyone can see their videos.
- Admins can choose to restrict content to be private or unlisted.
  - A private video can only be seen by you and the users you select. The video won't appear on your channel or search results and will be invisible to other users.
  - An unlisted means that only people who have a link to the video can view it. Unlisted videos don't show to viewers in the Videos tab of your channel page. Unlisted videos don't show up in YouTube's search results unless someone adds your unlisted video to a public playlist
  - More information about privacy settings can be found here: https://support.google.com/youtube/answer/157177?hl=en-GB&ref_topic=2946312
- Choosing to upload private or unlisted videos gives schools/settings control over who can see their content. Many schools/settings choose this approach initially. It does require administration work and schools/settings will need to regularly review the account.
- Restricting videos can be a downside if the school/setting wants to share learning etc. on a wider scale.
- Admins can also use tools to disable, moderate or remove comments posted on videos. It is recommended that schools/settings disable or moderate comments.
  - More information about this can be found here: https://support.google.com/youtube/answer/111870?hl=en-GB&ref_topic=2946312

Can we involve children aged 12 or under in using an official YouTube channel?

- YouTube's age limit is for children aged 13 and over, so it is inappropriate to use an official YouTube channel to directly communicate or inform children under 13.
  - o In many cases the school/setting will not be using YouTube to directly target communication with children but to share pupils work or events.
  - o It must however be acknowledged that if children are aware they are appearing in videos posted publically on YouTube then there is a significant chance they will choose to actively seek the content out. This could potentially place them at risk of being identified, for example if a pupil comments on the video and name themselves or others.
- When posting content involving pupils or their work on YouTube then schools/settings will need to appropriately assess the decision, considering the potential benefits and risks. Schools/settings will need to demonstrate that all reasonable precautions have been taken to reduce the risks of children being identified or placing themselves at risk.
- Schools/settings will also need to ensure that information can be accessed in other ways e.g. Facebook, Twitter, school website or learning platform for those not wishing to engage with Twitter.

What should we avoid posting on an official YouTube channel?

- Admins must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Admins should ensure the image policy is followed at all times.
- Leaders must ensure there is a clear procedure for admins to follow if there is a concern, for example reporting to the Designated Safeguarding Lead.
  - o Admins should not engage in public debates if opinions or concerns are raised.
  - o Admins should be cautious when deleting comments, unless they contain credible threats or offensive comments. Opportunities to engage with parents/carers and demonstrate that the school/setting listens to the community might be missed if legitimate comments are removed.
- Admins must not engage with any private messaging with children or parents/carers.

How do I block or report a YouTube account?

- Blocking someone on YouTube will stop them from making comments on your videos or Channel, and they won't be able to contact you through private messages either.
  - o To block a user visit their Channel page (which should have a URL similar to www.youtube.com/user/NAME)
  - o Access their "About" tab, click the **flag icon**
  - o Click **Block User**

- For further advice on how to "flag" content or users or report content to YouTube visit the YouTube safety centre: https://support.google.com/youtube/topic/2803138?hl=en-GB&ref_topic=2676378

Evaluating a YouTube channel

- Once your channel is live, ensure you set a timeframe in which to evaluate its success and have clear aims and objectives to help you measure this.
  - o If a concern occurs, revisit your training and policies and identify any lessons to be learnt.
  - o Involve all members of the community in reviewing the success (or not) of the YouTube channel – have they had a good or bad experience and do they have any constructive comments or views to help inform you?

Acknowledgements

This document is the work of the Kent Online Safety Strategy Group.

Additional material has been used and developed with thanks to the following organisations:

South West Grid for Learning
London Grid for Learning
Somerset eLiM
UK Safer Internet Centre
Childnet
CEOP

Using Social Media in Educational Settings