NAHT
FOR LEADERS, FOR LEARNERS

ADVICE & GUIDANCE

Social networking and online safety in schools

Social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuous personal development (CPD). We see social media replacing email as a means of communication and the increasing ownership of smart phones and the developments in tablet technology are key drivers.

What are the 'troubles' associated with new technology? When pupils first brought mobile phones to schools, theft was sometimes an issue. As technology advanced and video capacity developed, there was the issue of inappropriate filming. A further problem was the use of phones in the event of disputes in the playground or to call parents. The net effect was a perception that technology equated with 'trouble'.

It could be suggested that a more constructive and perhaps more challenging approach is to look for ways of managing the problems that can emerge. Key to this is having a clear understanding of what the potential pitfalls are and identifying proactive approaches to reduce the risk of incidents occurring.

Technological advances can offer significant benefits to modern teaching and learning. The government's policy of redefining ICT as 'computing' offers the opportunity to debate subject content. It can also be seen as recognition that the use of technology in the process of teaching and learning is largely accepted.

This guidance follows a risk assessment and management approach and throughout it will signpost you to external resources; these are by no means exhaustive but simply amount to those that have been drawn to our attention.

You may also find a resource produced by Kent County Council to be of use in approaching this matter:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety

Cyberbullying – an overview

The DFE has issued non-statutory advice for all schools on how to protect all staff from cyber-bullying and on how to deal with the problem.

Cyberbullying should be handled in the same way as all other forms of bullying. It is important to make it clear that the cyberbullying, whether by pupils, parents or colleagues is as unacceptable as bullying among pupils in the playground.

Schools can support parents to show children how to engage with social media in a safe and responsible manner. Advice can be given in a school newsletter, at a parents' evening or by signposting them to other support sources. Creating a good school-parent relationship with an atmosphere of trust encourages parents to raise concerns appropriately. Policies should make it clear that it is as unacceptable for pupils, parents or colleagues to denigrate or bully school staff via social media as it is to do so face to face.

School staff

School staff are in a position of trust; the expectation is that they will behave in a professional manner at all times.

To help protect reputations online, staff should:

- make sure they understand the school's social media policy;
- not leave computers or other devices logged-in when unattended;
- preferably use a pin or passcode on mobile phones or similar devices in case they are lost or stolen;
- be familiar with the privacy and security settings of social media apps used and keep them up to date; [the UK Safer Internet Centre website's reputation page has more information: www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation];
- be aware that their reputations can be harmed by what others share about them online - for example, being tagged in inappropriate posts, videos or photographs;
- consider their own conduct online - some behaviour could breach the employment behaviour policy or code of conduct;
- discuss issues with colleagues, close family and friends to ensure they have appropriate privacy and security settings;
- not accept friend requests from past or present pupils;
- not give out personal contact details. If pupils need to contact a member of staff they should be given the school's contact details;
- ask for a school mobile phone to be issued to staff on school trips rather than using a personal phone; and
- keep their school email address for school business and their personal email address for private communications.

If online bullying occurs

- Do not respond to bullying incidents, report them appropriately and seek support from an appropriate manager
- Take screen shots of messages or web pages and record the time and date
- The school mediation and disciplinary procedures can be applied if the perpetrator is known to be a current pupil or colleague
- If the perpetrator is an adult, they should be invited to a meeting with a senior member of staff to address concerns. If the complaint is reasonable, they

should be informed of the appropriate way to raise this and request that the person removes the offending comments
- If the person refuses to remove the comments, the matter can either be reported to the social networking site if it breaches their terms or guidance and advice can be sought from the local authority's or relevant body's legal team. Other agencies such as the UK Safer Internet Centre www.saferinternet.org.uk/ can also provide advice
- Online harassment may amount to criminal conduct; if the comments are of a sexual nature, sexist, threatening, constitute a hate crime or are abusive, then consideration should be given to contacting the police

You could obtain screenshots of offensive material for your own records, however, be cautious about using this material, especially if you intend to present the screenshots to parents as evidence. It is important that you do not do anything unlawful with the data, that you handle it confidentially and that you consult with any third party involved before using it.

Employers have a duty of care to staff and no-one should feel victimised in the workplace. Support can be sought from the senior management team and from union representatives if appropriate.

The UK Safer Internet Centre, which has developed strategic partnerships with internet industry key players, offers a free service for those working with children and young people: The Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline.

This provides advice, mediation and signposting to resolve e-safety issues. The helpline can seek direct resolution with the safety and policy teams at Rate My Teacher, Ask.FM, Google, Facebook, Twitter, YouTube, Tumblr and others when appropriate.

Schools

School policies and practices to combat bullying should also include cyberbullying. It is an employer's duty to look after employees' mental and physical health.

Clear guidance should be developed to help protect everyone and sanctions should be consistent and appropriate. Effective communication and discussion needs to take place with staff, pupils and parents. Reporting procedures [responsibilities and routes] should be clear and understandable.

Acceptable use policies

A clear 'acceptable use policy' that addresses cyberbullying should be in place in all schools for pupils and staff members. This should include:

- rules on the use of school equipment, in or outside school hours and on or off site;

- guidelines on acceptable behaviour for employees and pupils within and outside of school;
- an expectation that the school will respond promptly to incidents reported by staff and provide support;
- efforts to approach the social networking site to request the removal of inappropriate material. However, providers may only accept requests from victims. The school should take action if the material is on a school website or has been sent through the school's email; and
- if the victim approaches the provider directly, the school should provide support.

Schools and professionals working with parents can deliver their own internet safety sessions by using the training programme established by The Parent Zone.

Facebook has launched the Bullying Prevention Hub https://en-gb.facebook.com/safety/bullying and produced a support sheet specifically for teachers entitled 'Empowering Educators'.

Removal of offensive content

If those responsible for offensive or inappropriate online content are known, the school should ensure they understand why the material is unacceptable and request that they remove it.

Most social networks have mechanisms in place where content that breaches their terms can be reported. If the responsible person is not identified or does not take down material as requested, the victim can use the tools directly on the site to report inappropriate content.

It is important to be clear about the location of the content before contacting the provider, such as by taking a screen shot of the material including the web address. If the material to be taken down is not illegal, it will be necessary to point out clearly how it breaks the terms and conditions of the site. If the content is suspected to be illegal, the police should be contacted.

The screenshot should also be taken in the presence of a colleague and the whole process documented (for example, the screenshot should be signed and dated by more than one person).

It is likely that a screenshot taken from Facebook, for example, falls under the definition of 'personal data', defined as:

"Data which relate to a living individual, who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual" (1998 Data Protection Act).

Handling screenshots must comply with the first data protection principle, set out below. In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;

  Do not use the data in ways that have unjustified adverse effects on the individuals concerned; be transparent about how you intend to use the data and give individuals appropriate privacy notices when collecting their personal data;

- handle people's personal data only in ways they would reasonably expect;

- make sure you do not do anything unlawful with the data.

(From the Information Commissioners Office)

Access to inappropriate material

As technology has become increasingly ubiquitous, the ability to monitor usage by children and young people becomes more of a challenge. NAHT has become increasingly concerned about reports that younger children are accessing pornographic and violent material and has been working with a number of bodies to raise awareness of this issue and press for action.

Given the logistical difficulties of the above, NAHT has taken the view that a risk assessment approach to this matter ought to have education at its core and that this should be an explicit aspect of PSHE provision for all ages.

On a practical level, NAHT's advice is that schools work with parents to raise awareness of this issue.

NAHT recommends the CEOPS resource for parents and carers: www.thinkuknow.co.uk/parents. This may be the best 'first port of call' because it enables a school to choose resources and approaches best suited to its context.

In recent years, there has been mounting concern about 'sexting'. This is the practice of people exchanging intimate and compromising messages, images and videos of themselves via social networking or through mobile messaging services. The UK Safer Internet resource includes a parental guide: *A parent's guide to dealing with sexting*. This is linked to a document produced for schools: *Sexting in schools: advice and support around self-generated images*. This is strongly recommended and NAHT supported its production:

www2.kirklees.gov.uk/childrenandfamilies/learning/documents/subjects/Esafety/Policy-Guidance/Sexting-Self-generated-Images-and-responding-to-incidents/Sexting-Booklet.pdf

There may be an understandable tendency to regard this as a practice affecting secondary-aged pupils. However, those working in the field find instances of younger children being involved or being exposed to such material.

Appendix 1: E-safety parameters
From the new national curriculum programmes of study

Key stage 1	Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
Key stage 2	Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
Key stage 3	Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct, and know how to report concerns.
Key stage 4	Understand how changes in technology affect safety, including new ways to protect their online privacy and identity and how to report a range of concerns.

Extract from Ofsted briefing on inspecting e-safety; the entire document can be located here:

www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies

Key features of good and outstanding practice

Whole school consistent approach	• All teaching and non-teaching staff can recognise and are aware of e-safety issues • High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-safety mark) • A high priority given to training in e-safety, extending expertise widely and building internal capacity • The contribution of pupils, parents and the wider school community is valued and integrated
Robust and integrated reporting routines	• School-based reporting routes that are clearly understood and used by the whole school, for example, online anonymous reporting systems • Report abuse buttons, for example, CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support

Staff	• All teaching and non-teaching staff receive regular and up-to-date training • One or more members of staff have a higher level of expertise and clearly defined responsibilities
Policies	• Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors • The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying • The e-safety policy should incorporate an acceptable usage policy that is understood and respected by pupils, staff and parents
Education	• An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety • Positive rewards are used to cultivate positive and responsible use • Peer mentoring programmes
Infrastructure	• Recognised internet service provider (ISP) or regional broadband consortium (RBC) together with age-related filtering that is actively monitored
Monitoring and evaluation	• Risk assessment taken seriously and used to good effect in promoting e-safety • Using data effectively to assess the impact of e-safety practice and how this informs strategy
Management of personal data	• The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998 • Any professional communications between the setting and clients that utilise technology should: o take place within clear and explicit professional boundaries; o be transparent and open to scrutiny; and, o not share any personal information with a child or young person.

Indicators of inadequate practice

Inadequate	• Personal data is often unsecured and/or leaves school site without encryption • Security of passwords is ineffective, for example, passwords are shared or common with all but the youngest children

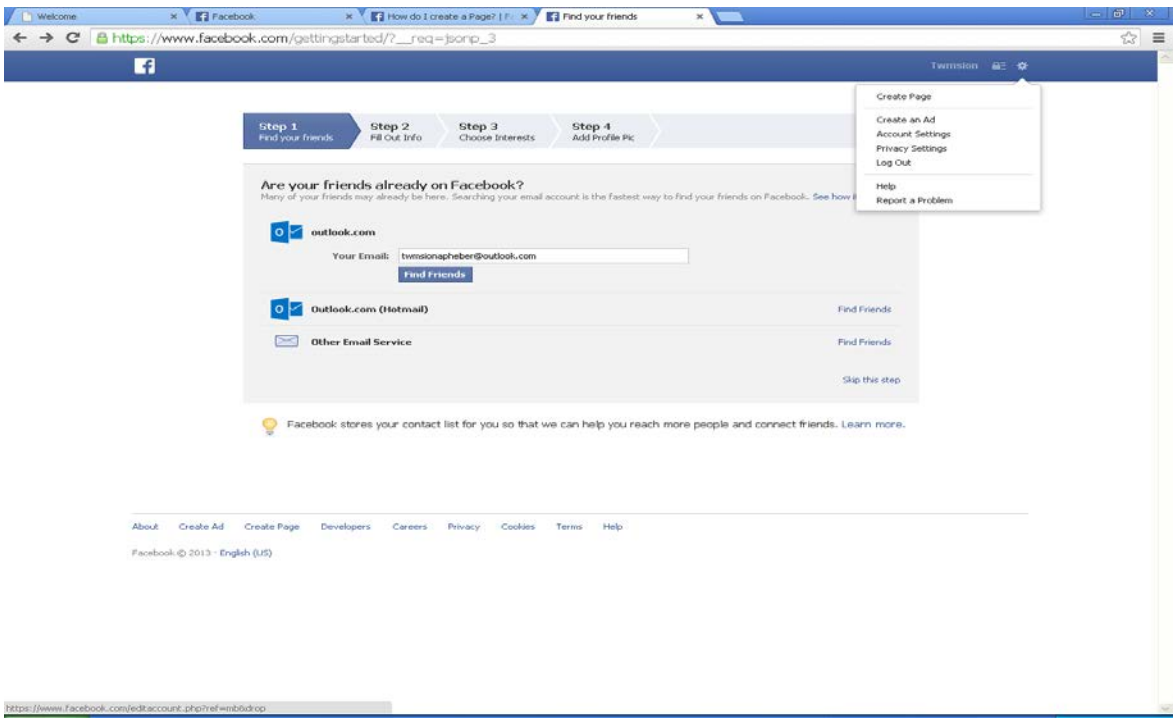
	• Policies are generic and not updated • There is no progressive, planned e-safety education across the curriculum, for example, there is only an assembly held annually • There is no internet filtering or monitoring • There is no evidence of staff training • Children are not aware of how to report a problem

Appendix 2: Procedures for reporting abusive content on social media sites

Members are strongly advised to record as much information about abusive and inappropriate content before seeking its removal. This includes taking screenshots and recording URLs

Facebook

- There is a button on the top right corner of the page. Selecting it will produce a menu:



- The last option is ‘report a problem’. Clicking on this will produce three options, the third of which is ‘you can also report abuse, spam and policy violations’
- Clicking on this will bring up a page that contains a range of options covering most eventualities
- It is a common complaint that Facebook is slow to respond. Its criteria for deciding whether content is unacceptable is based on its ‘community standards’ (www.facebook.com/communitystandards)
- Members may wish to use this as a checklist before seeking to have material removed both as a means of assessing Facebook’s likely response and to be able to fully contextualise the complaint and request for removal

Twitter

Twitter provides an intuitive guide to dealing with abusive content and other inappropriate usage at https://support.twitter.com/articles/15789-how-to-report-violations.

This link brings up a page that outlines Twitter’s definitions of various categories of misuse. The following relates to ‘abusive behaviour and violent threats’:

When reporting abusive behaviour on Twitter, please provide the following:

- Description of problem, including length of time the abusive behaviour has been happening
- Tweet URLs (to find the exact link of a Tweet, please review this article)
- Tweet text (copy and paste the text of the Tweet into the form)
- Your email address

Please note: If you believe you may be in danger, consider contacting the police in addition to reporting the content to Twitter.

To report abusive behaviour on Twitter, click here.

For more information about Twitter’s abusive behaviour policy, click here.

For more information about reporting abusive behaviour on Twitter, click here.

- The link also includes sections on child sexual exploitation and pornography.
- For a more general resource on factors related to Twitter in schools an e-safety advisor resource is located at www.esafety-adviser.com/twitchy_twitter

You Tube

- You Tube has clear community guidelines which, as with Facebook, provides a good indication of how seriously it will respond
- The site is open in stating that it does not have the resources to monitor every uploaded video. They therefore rely on users reporting what is considered to be unacceptable material by means of a 'flagging system'. If a video is flagged, moderators review the content
- The flagging system works by means of the last button on the right hand side under the video player

- More specific reporting of unacceptable content can be done at: www.youtube.com/reportabuse

There are parallels with Facebook in that the community guidelines provide the criteria. Central to this in the case of You Tube is its definition of 'harassment'.

Ask.fm

Ask.fm is a site that allows individuals to upload a profile and others to subsequently post questions relating to its content. There have been numerous concerns (for example, http://metro.co.uk/2013/08/19/ask-fm-reveals-new-safety-features-following-death-of-hannah-smith-3929485/) about inappropriate content. The following link outlines how to deal with abusive content but does not detail how content can be taken down: www.webwise.ie/AskfmGuide.shtm.

Snapchat

This is an app that enables transmission of photographs and/or videos. The technology is such that it only remains visible for up to 15 seconds. The app has developed a reputation in some quarters (although denied by Snapchat itself) of being the 'sexting' app.

The following link helps to deal with incidents involving Snapchat in addition to the sexting links provided earlier in this document: www.connectsafely.org/wp-content/uploads/snapchat_guide.pdf.

WhatsApp

WhatsApp messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS. You cannot contact WhatsApp to remove content but you can block the contact by selecting them and choosing 'block' from the options.

Appendix 3: Model letter inviting a parent to attend a meeting to discuss offensive or threatening comments made online

Dear [parent/carer name(s)],

It has been drawn to my attention that you may have recently made comments online on Facebook [or other site] relating to an event [or events] you believe to have taken place in this school.

I am very concerned about the tone of comments made and their abusive and threatening nature [substitute more appropriate adjectives if necessary]. It is important that if you have concerns that you raise them with me in the first instance.

To move forward we should meet to discuss this matter informally in an open and constructive manner. I invite you to contact me at your earliest convenience to arrange an appointment. My colleague [insert name and role] will be present to act as note-taker and you may also be accompanied by a family member or friend. I must emphasise, however, that the conversation must remain confidential.

I look forward to hearing from you.

Yours sincerely,

[Name]
[Role]