MONKTON INFANTS SCHOOL

Aiming High!

Social Media Policy

SOCIAL MEDIA POLICY

STATEMENT OF INTENT

Monkton Infants School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

Monkton Infants School is committed to:

- Encouraging the responsible use of social media in support of the school/academy’s mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

KEY ROLES AND RESPONSIBILITIES

- The governing body has overall responsibility for the implementation of the Social Media Policy and procedures of Monkton Infants School.
- The governing body has responsibility for ensuring that the Social Media Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- The governing body has responsibility for handling complaints regarding this policy as outlined in the school’s Complaints Policy.
- The Headteacher will be responsible for the day-to-day implementation and management of the Social Media Policy and procedures of Monkton Infants School.
- Staff, including teachers, support staff and volunteers, will be responsible for following the Social Media Policy and for ensuring pupils do so also. They will also be responsible for ensuring the policy is implemented fairly and consistently in the classroom.
- Parents and carers will be expected to take responsibility for the social media habits of their child/children at home.
- Parents and carers will be expected to promote safe social media behaviour.

DEFINITIONS

Monkton Infants School defines “social media” as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:

- Blogs.
- Online discussion forums, such as netmums.com.
- Collaborative spaces, such as Facebook.
- Media sharing services, such as YouTube.
- ‘Micro-blogging’ applications, such as Twitter.

- Monkton Infants School defines “cyber bullying” as any use of social media or communication technology to bully an individual or group.

- Monkton Infants School defines “members of the school community” as any teacher, member of support staff, pupil, parent/carer of pupil, governor or ex-pupil.

STAFF TRAINING

At Monkton Infants School, we recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.

Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.

Teachers and support staff will receive regular and ongoing training as part of their development.

PUPIL EXPECTATIONS

Pupils are responsible for following the school rules and will be expected to follow requests from teachers.

SOCIAL MEDIA USE - STAFF

- School social media passwords must never be shared.
- Teachers may not access social media during lesson time, unless it is part of a curriculum activity.
- The use of smart phone technology is outlined in our Mobile Phone Policy.
- Teachers may use social media during their break times.
- Members of staff should avoid using social media in front of pupils.
- Members of staff must not “friend” or otherwise contact pupils or parents/carers through social media.
- If pupils or parents/carers attempt to “friend” or otherwise contact members of staff through social media, they should be reported to the Headteacher.
- Members of staff should avoid identifying themselves as an employee of Monkton Infants School on social media.
- Members of staff must not post content online which is damaging to the school or any of its staff or pupils.
- Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

- Members of staff should be aware that if their out-of-work activity brings Monkton Infants School into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Headteacher.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.
- Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

SOCIAL MEDIA USE – PUPILS / PARENTS AND CARERS

- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Pupils and parents/carers must not attempt to “friend” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the Headteacher.
- If members of staff attempt to “friend” or otherwise contact pupils or parents/carers through social media, they should be reported to the Headteacher.
- Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils and parents/carers must not post content online which is damaging to the school or any of its staff or pupils.
- Pupils at Monkton Infants School must not sign up to social media sites that have an age restriction above the pupil’s age.
- If inappropriate content is accessed online on school premises, it must be reported to a teacher.

BLOCKED CONTENT

- Attempts to circumvent the network’s firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Inappropriate content which is accessed on the school computers should be reported to the Headteacher so that the site can be blocked.

CYBER BULLYING

- At Monkton Infants School, cyber bullying is taken seriously.
- Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from their line manager or senior staff member.
- Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.

- Where the perpetrator is an adult, in nearly all cases, the Headteacher should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.
- As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

BE S.M.A.R.T ONLINE

We encourage pupils to take a SMART approach to social media behaviour:

- Safe – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.
- Meeting – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.
- Accepting – We advise that pupils only open emails and other forms of communication from people they already know.
- Reliable – We teach pupils about the dangers of believing everything they see online.
- Tell – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

RISK ASSESSMENT – SOCIAL MEDIA

WHAT IS SOCIAL MEDIA?

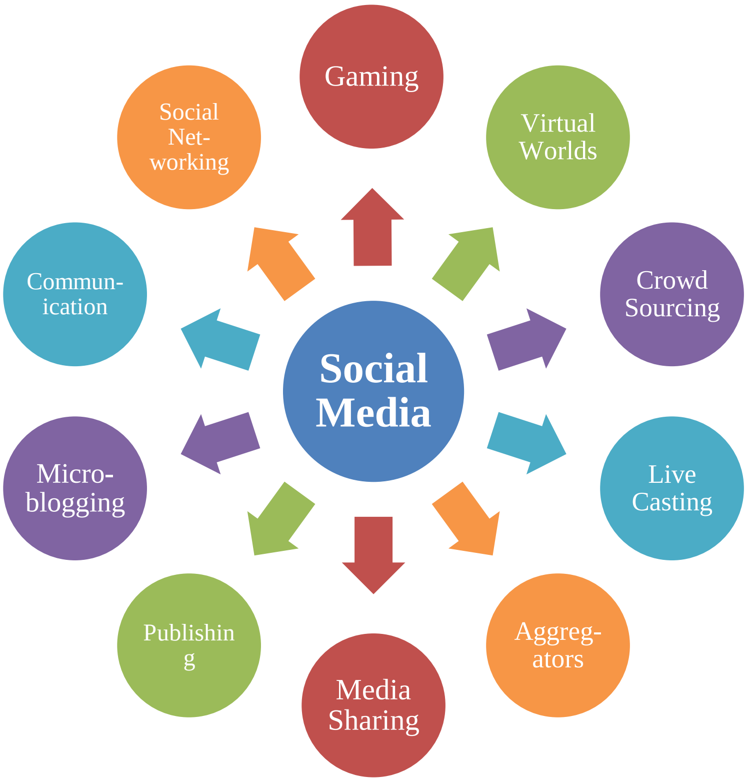
According to Wikipedia, social media are computer-mediated technologies that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. The variety of stand-alone and built-in social media services currently available introduces challenges of definition. However, there are some common features:

Social media are interactive Web 2.0 Internet-based applications
User-generated content, such as text posts or comments, digital photos or videos, and data generated through all online interactions, are the lifeblood of social media
Users create service-specific profiles for the website or app that are designed and maintained by the social media organization
Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals and/or groups.

Social media use web-based technologies, desktop computers and mobile technologies (e.g., smartphones and tablet computers) to create highly interactive platforms through which individuals, communities and organizations can share, co-create, discuss, and modify user-generated content or pre-made content posted online. They introduce substantial and pervasive changes to communication between businesses, organizations, communities and individuals. Social media changes the way individuals and large organizations communicate.

Social Media may be classified into different areas of collaboration and sharing.

CLASSIFICATION OF SOCIAL MEDIA APPLICATIONS



This is just one way to map out the social media landscape. Social networking also provides some overlap. For example, Facebook provides a chat feature that would fall under conversation apps. Facebook also provides photo sharing where users can post photos and even tag people in the photos. Facebook as a social networking site integrates many of the other social media categories into one stop shopping.

WHAT IS THE RISK?

When examining different reports and articles regarding social media risks, there are two common risks that are mentioned often: reputation damage and data leakage. Both of these risks are related in one way, as data leakage can cause reputation damage.

Unlike traditional news media, in social media anyone can blog and post information about anyone or any organization. Facts may go unchecked. An organization might be able to exert some control over their employees, but any disgruntled or unsatisfied parent or pupil can have the opportunity to sound off. Removal of an offending post may be difficult or impossible to achieve.

The other risks of the use of Social Media in schools are:

Financial Risks – releasing information about financial situation that isn't normally public, or exposure to add on purchasing. Also if marketing opportunities are missed through not using social media.

Information Security & Privacy – allow access to data or information that pertains to the running of the school or about personnel at the school. Sharing passwords or not changing them frequently. Infection to the school network from a virus, malware etc downloaded from a social media site.

Legal & Employment Risks – if information from a social sharing site is used in disciplinary or hiring situation.

Operational Risks - A person of authority posts content that is deemed to be hostile, discriminatory or offensive that is viewed by employees. Employee overuse impacting on productivity.

MAJOR RISKS OF USING SOCIAL MEDIA

	Risk	Threat	Vulnerability	Likelihood	Impact
Reputation Damage	Reputation	High	High	High	High
	Representation – fake sites	Low	High	Low	High
	Harassment	High	Medium	Medium	High
Information security and privacy	Information Leakage	Low	Low	Low	High
	Data Loss	Low	Low	Low	High
	Privacy	Low	Low	Low	High
	Passwords	Low	Low	Low	Low
	Permanence of content	Medium	Medium	Low	Medium

Operational	Piracy and Infringement	Low	Low	Low	Low
	Content and ownership	Medium	Medium	Low	Low
	Copyright	Medium	Medium	Low	Low
	Virus and Malware	Low	Low	Low	Low
Financial	Purchasing from applications and games	Low	Low	Low	Low
	Scam and phishing	Low	Low	Low	Low
Legal and Employment	Employment	Low	Low	Low	Low
	Overuse	Low	Low	Low	Low

SOCIAL MEDIA RISK ASSESSMENT FOR SCHOOLS

Hazard	Who it will affect	Control Measures to Reduce Risk	Further Action Necessary	Risk Rating Low/Med/High
Reputation	All	Small number of named members of staff to have responsibility of posting to social media sites. Monitor any posts made about the school and be proactive in asking for removal if defamatory. If staff can post to school website some sites are automatically linked to post to other social media sites. Staff should be mindful of this.		High at all levels.
Representation	All	Monitor web for sites being created as school or members of staff. Report any suspicious activity to the social media site concerned.	Consult legal team if libelous.	Low Threat and likelihood, high vulnerability and impact.
Harassment	All	Encourage disclosure of any harassment. Meet with affected parties if possible. Ask for apologies and removal of posts. Revision of AUP's for all stake holders. Meet with Union representative if staff member is involved. Contact police if situation is not resolved.	E Safety training and awareness for all stake holders.	High threat and impact, medium vulnerability and likelihood.
Information leakage	All	No personal, financial or sensitive material to be posted online on an unsecured site. All students to have permissions for work and images to be posted online. Refer to Data Protection policy.		Low, but high impact
Data loss	Selected members of staff	Data should be hosted on a secure site not on social media. Refer to Data Protection policy.		Low
Privacy	All	No information relating to personal details to be posted online. Ensure privacy settings on social media sites are set at the highest possible		Low but high impact

		level. Regularly check settings. Where possible make the school social media site impersonal and not linked to a staff member's personal profile.		
Passwords	Selected members of staff	Only selected members of staff to have log ins to social media sites. Make passwords robust. Change passwords according to protocol in staff policy. Passwords not to be shared or told to another user.		Low but high impact
Permanence of content	All	On those sites that the school control such as their school website, older posts can be archived or removed. This does not mean they have disappeared from the web entirely as the pages may have been archived on such sites as Wayback machine. On sites such as Facebook and Twitter etc. content ownership is with the site .		Medium but low likelihood
Piracy and infringement	All	All content posted should comply with legal regulations.		Low
Content and ownership	All	Content ownership is with social media sites such as Facebook or Twitter and users agree on signing up to relinquish their control of content.		Medium threat and vulnerability, low likelihood and impact
Copyright	All	All content posted should comply with copyright regulations.		Medium threat and vulnerability, low likelihood and impact
Virus and Malware	All	Don't accept any files or friend requests. Be wary of shortened URL's. Don't download any multimedia content or applications from a social media site.	Ensure virus checking software is enabled, up to	Low

			date and running.	
Purchasing from applications and games	All	Don’t download any games or applications from a social media site.		Low
Scam and phishing	All	Don’t complete online forms, surveys or supply log in details. Don’t share posts or competitions from commercial sites.		Low
Employment	Selected members of staff	Don’t advertise vacancies on unsecured social media sites.		Low
Overuse	All	Refer to Acceptable Use Policy.		Low