

=====
Crudgington Primary School Staff Social Media Policy
=====

=====
September 2019
=====

=====
ALL STAFF
=====

Introduction

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views
- **contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying. (in line with Keeping Children Safe in Education – September 2019)

The widespread availability and use of social media applications such as Facebook and Twitter, bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. To capture the benefits offered by social media, the School may explore and implement its use for school improvement and educational purposes.

Working in a school requires us all to maintain professional boundaries in all forms of communication whether or not it involves electronic/digital technology. This is vital to maintain public trust and appropriate professional relationships with students. Our conduct inside or outside of work should not lead us to blur or cross those professional boundaries.

This policy and the principles below are to help staff and individuals avoid the downside risks of using social media. The principles apply to any approved use of social media communication within the school or to personal use of social media outside of school.

Application

This document applies to all staff, including agency/supply staff, volunteers, governors or anyone working within the school and using the school's systems and equipment whether on or off the premises. The policy may also apply to former employees in certain circumstances. The use of the word 'individuals' in this document includes this range of people.

The policy and principles should be read in conjunction with the School's policies on Online Safety, Acceptable Use of ICT and the Staff Code of Conduct.

Social Media – What is it?

In this document, social media means electronic communication software, applications (including those running on mobile devices including texting, SMS, and videos), email and web sites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, Instagram, YouTube, as well as online discussion forums, blogs, and the use of webcams.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, The Safeguarding Vulnerable Groups Act 2006, the Malicious Communications Act 1988 and other legislation.

Access to Social Media Sites using School Equipment/Systems

With the exception of communication sites created by or approved by the school for internal use, the School does not allow access to social networking websites from its computers or systems within the school day.

Key Principles when Using Social Media Sites

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account and the curriculum may require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning. However, when using social media, the boundaries between professional and personal can become more blurred and users can unwittingly or wittingly publish things they may later regret. Published items can be capable of more than one interpretation but once published the damage may not be recoverable.

The golden principles

An individual is under a duty to:

- Maintain proper professional boundaries with students, parents and carers even when students, parents or carers initiate electronic interaction
- Before posting items or communicating in social media to consider seriously whether the item would be said in public or shown in public or written for the public to read. If not, or if there is some doubt then it should not be posted because you may not be able to control who sees the information and how they interpret it
- Be particularly aware of the guidelines when staff have external friendships with parents/carers.

An individual is under a duty not to:

- Disclose confidential information without express authority especially about students, parents or carers, staff, voluntary or other workers at the school nor breach their right to privacy
- Engage in posts or activities which are detrimental to maintaining effective working relationships between individuals 'working' at the school
- Bring the reputation of the school into disrepute
- Engage in activities which compromise, or might be seen to compromise, the professional standards of teaching or the professional standards applicable to support staff
- Share information with students or parents/carers in any environment that they would not willingly and appropriately share in a school or school related setting or in the community
- Post comments which incite others to make discriminatory or other professionally unacceptable comments
- Post school logos or similar images that may lead readers of posts etc. to believe the individual is speaking on behalf of the school.

Items placed on social networking sites will be regarded as having been posted in the public domain. Thus, it is very important to be careful when using social media personally.

Effective practices when using social media sites

Members of staff should:

- Use caution when posting information on social networking sites and other online forums
- Refrain from identifying themselves as working for the school as posted content could bring the school into disrepute

- Take care that their interaction on social media does not damage working relationships between members of staff, students at the school, their families and other stakeholders and/or working partners of the school
- Maintain professional standards by communicating with student & parents/carers electronically at appropriate times of the day and through established education platforms (for example, a web page dedicated to school programme, project or class rather than via a personal profile)
- Avoid exchanging private texts, phone numbers, personal email addresses or photos of a personal nature with students/parents or carers
- Decline student/parent initiated 'friend' requests and not issue 'friend' requests to students/parents nor communicate with students/parents on any social network site or similar website or forum
- Maintain a formal, courteous and professional tone in all communications with students/parents to ensure that professional boundaries are maintained
- If posting an item about an aspect of the school, for which you have express permission from the Headteacher, make it clear that any personal views are not necessarily those of the school
- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

Manage the privacy and security settings of your social media accounts. Privacy settings can shift and change without notice. Check the settings frequently.

- Ensure that privacy settings for content/photos are set appropriately and monitor who can post to your social media locations and view what you post. You should not allow students to view or post on those locations
- Protect yourself from identity theft by restricting the amount of personal information that you give out. Be cautious about posting detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords and enable personal details to be cloned for fraudulent acts etc and grooming.

The following activities must not be undertaken:

- Bullying and harassment – such conduct against any colleagues via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the schools' normal bullying and harassment and/or disciplinary policies and may be treated as a criminal offence in certain circumstances
- Incitement of racial or religious hatred or similar activities – these may lead to criminal investigations and penalties
- Posting libellous statements – an individual may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by an employee could mean the school is vicariously liable for

defamatory statements if carried out in the normal course of employment, even if performed without the consent or approval of the school. Similarly, making such statements on your own initiative and not at work could mean you face legal action

- Grooming students or similar activities to develop an inappropriate relationship(s)
- Bring the school's reputation into disrepute
- Compromising the security of the school's systems
- Breaching confidential information about the school or any of its students, staff, governors, volunteers or other individuals associated with the school. Don't publish anything that might allow inferences to be drawn which could embarrass or damage a student, employee, governor, volunteer or supplier.
- Breaches of copyright or other similar infringements – passing on text, photos etc; may infringe the owner's copyright. Always ensure that you have the permission of the owner

The school takes the matters above seriously and disciplinary action will be taken. If substantiated, the outcome may include dismissal. A very serious view will also be taken of any individual who ignores or wilfully or carelessly carries out actions or omits to act which results in breaches of the instructions and advice contained in this policy and the result is for example, undermining effective working relationships, professional boundaries between individuals and student similar examples in this policy.

Feeling aggrieved or concerned about matters at work

When you feel that unfair decision has been made or that malpractice is occurring, what can you do?

What you should not do is post your feelings on-line, which are likely to be impulsive, inappropriate or heated comments. Those may lead you into being part of the problem. Instead you can use several routes:

Whistle blowing procedure - for allegations of organisational malpractice or corruption – see the Whistle Blowing Policy. Following this procedure provides protection against dismissal and other sanctions if you disclose matters in the ways set out in the procedure. Posting comments first will mean you may forfeit your legal protection.

Grievance procedure - if you feel aggrieved by a decision at the school that affects you personally.

Dealing with inappropriate contact or material/comments

If an individual becomes aware of inappropriate material/comments they should notify the Headteacher or Assistant Headteacher as soon as possible, and if possible, provide print outs of the comments made. If a student makes 'social' or inappropriate contact with an

employee or person, the individual must notify the Designated Safeguarding Lead as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a pupil, the incident must be notified to the Designated Safeguarding Lead as soon as possible. The school can then deal with the situation as appropriate. Refer to the school's Safeguarding Policy if the incident gives rise to potential or actual safeguarding concerns.

Final Reminders

As noted at the outset, social media is a useful means of communication. Because of its ease of access and familiarity, it can lead us to unwittingly overstep the boundaries of professional standards and conduct towards students or work colleagues.

When using social media, individuals should remember that the school is a public body and that we are subject to various expectations.

Please remember that when using such media to:

- Ensure that no information is made available that could provide a person with unauthorised access to the school, its systems and/or any confidential information.
- Not post any confidential information regarding the school on any social networking website.

We ask all individuals to consider the following before posting information or images on social networking sites:

- Think carefully before posting information – would you want the person concerned or your employer or potential employer to see it?
- Review your posted information regularly – what may have seemed like a good idea at the time may not seem such a good idea some months or years later.



Mobile Phone

Staff are not permitted to contact parents, carers or children via mobile devices. Parental numbers must not be stored in your mobile phone as they may give access to linked apps such as WhatsApp



Text Messages

Staff are not permitted to contact parents, carers or children via text message. Parental numbers must not be stored in your mobile phone as they may give access to linked apps such as WhatsApp



WhatsApp

Staff are not permitted to contact parents, carers or children via WhatsApp. This includes being a member of group chats and any parent created school focussed group chats.



Instagram

Staff are not permitted to contact parents, carers or children via Instagram. Instagram accounts should be private so no parents, carers or pupils should be able to access your feed. Any requests to follow you by a pupil should be reported to a member of the SLT immediately.



Facebook

Facebook accounts should be private and have the strongest privacy settings enabled. Staff should not have parents/carers or children as friends (save for when pre-existing friendships exist). Any friend requests by a pupil should be reported to a member of the SLT immediately. Staff should not participate in school focussed groups e.g. PTA and class pages.



Facebook Messages

Staff are not permitted to communicate with parents, carers or children through Facebook Messages. Any messages received by a pupil should be reported to a member of the SLT immediately.



Emails

Staff are not permitted to contact parents using their school email account. Not only is this inappropriate it risks disclosing other internal staff email addresses. If staff receive a direct email from a parent, they should send the response to the school office to be sent from the school email address and tell a member of the SLT.