Grangetown Primary School

Use of Social Media Policy

Author	Grangetown Primary SLT
Date	September 2017
Review Frequency	1 year
Review Date	September 2018
Governor Approval	

Grangetown Primary School offers a positive, safe learning environment for its community, in which everyone has equal and individual recognition and respect. We celebrate success and are committed to the continuous improvement and fulfilment of potential in every child.

We encourage increasing independence and self-discipline amongst the pupils. Everyone within the school has an important role to play in sharing responsibility for the development of positive behaviour and attitudes.

Aims:

At Grangetown Primary School, we have high aspirations and ambitions for our children and we believe that no child should be left behind. We strongly believe that it is not about where you come from but your passion and thirst for knowledge, and your dedication and commitment to learning; your 'UMPHHHH' that make the difference between success and failure, and we are determined to ensure that our children are given every chance to realize their full potential.

This policy recognizes that new technology are an integral and growing part of everyday life and make an important contribution to teaching and learning opportunities. However, rapid evaluation of social networking technologies requires a robust policy framework and this policy aims to:

- Assist staff working with children to work safely and responsibly with the internet and other communications technologies and to monitor their own standards and practice.
- Give a clear message that unlawful and unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.
- Set a clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal and recreational use.
- Support safer working practice.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Prevent adults abusing or misusing their position of trust.

This policy applies to all staff who work in the school whether paid or unpaid. This includes members of the Governing Body, where Parent, Community or Local Authority Governors.

Background

Social networking and social media are communication tools based on websites or networks which allows you to share information or other material about yourself and your interests with groups of other people. These groups of people could be:

- People who are known to you (friends or colleagues)
- People you don't know who share common interests.
- Anyone who could find your comments through search engines

Context

This policy is concerned mainly about two types of social media activity:

- Your personal activity done for your friends and contacts, but not under or in the name of Grangetown Primary School.
- Activity carried out in the name of Grangetown Primary School, such as school blog, twitter, Facebook that represents the school, or that appears to represent the official views of the school.
- This policy is not about stopping you using or accessing such groups, but aims to ensure that your use of social media that does not harm the reputation of the school or school staff and ensure the interests of the children are supported.

Key Principles

The principles that underpin this policy are:

- Adults who work with pupils are responsible for their own actions and behaviour and must avoid any conduct which would lead any responsible person to question their motivation or intensions.
- Adults in the school must work and be seen to work, in an open and transparent way.
- Adults in the school must continually monitor and review their own practice in terms of the continually evolving world of social media and ensure that they consistently follow the guidance in this document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in social media that they have later regretted, because that information has harmed or put at risk themselves or others. This includes:

- Accidently posting personal or embarrassing information about themselves or others in a public forum or beyond the group information was originally intended for.
- Sharing information about yourself or others with people you don't know that could be used by someone to commit fraud or misrepresent the views of yourself or others (such as identity theft)
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and adults that you work with.
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.

This has led to people facing disciplinary actions, losing their jobs, being prosecuted or even imprisoned. This policy and guidance will make sure sites such as Facebook, Twitter, etc. and all other current and emerging technologies are a safe place.

Safer Networking Practice applies to current social networking sites such as Facebook, Twitter etc and all other current emerging technologies.

My Safer Social Networking Practice is broken down into:

- Things you must not do, because they are illegal, contrary to regulations or against school policy (such as professional boundaries)
- Things you should do to avoid risk to yourself or others
- Good practice things you should do to reduce the risk that information you put on social networking sites or media cannot later be used against you.

All staff and volunteers must adhere to and apply the principles of this document in all aspects of work. Failure to do so may lead to action being taken under the disciplinary procedure.

Monitoring

Social Network "Must Nots"

- Staff or volunteers must not make comments on behalf of the school or claim to represent the views of the school, unless they have explicit permission to do so.
- Staff and volunteers should never make a 'friend' of a pupil at the school where they are working on their social networking page and seek advice or the Headteacher, Deputy Head or ICT leader before becoming 'friends' with ex – pupils.
- Staff and volunteers should never use or access social networking pages of pupils.
- Staff and volunteers must not request, or respond to, any personal information from a pupil.
- Staff and volunteers should never post confidential information about themselves, the school, the governing body, the local authority, their colleagues, pupils. IF they are posting in an 'official' capacity they should not post confident information about members of the public.
- Staff and volunteers should not make allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or other school, or local authority. Doing so may results in disciplinary action being taken against them. If they have concerns about practices within school or actions or pupils or parents, they must act in accordance with the school Whistle- Blowing Policy.
- E-mail or text communications between staff member/volunteer and a pupil outside must not take place outside the agreed protocols (Acceptable use policy)

Social Networking "Shoulds"

- All adults, particularly those new to the school, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes photographs that may cause embarrassment to themselves and/or the school if they were to be

published outside of the site.

- In their own interests, adults with the school setting need to aware of the dangers of putting their personal information onto social networking sites such as addresses, home or mobile numbers. This will avoid the potential for pupils or their families or friends having access to staff outside the school environment. It also reduces the potential for identity theft by third parties.
- Some social networking site and other web based sites have fields in the user profile for job title etc. As an employee or volunteer of the school and particularly if you are a teacher or teaching assistant, you should not out on any information onto the site that could identify either your profession or school where you work. In some circumstances this could damage the reputation of the school and the profession. If it is a work-based site where you are required to provide this information, you must obtain permission of the Headteacher or Deputy beforehand.
- Staff and volunteers should keep their personal phone number, work login or password and professional email addresses private and secure. Where there is a need to contact pupils or parents the school email address and/or telephone should be used. If, with permission, telephone call are made from a personal phone (landline/mobile) the telephone number the call is being made from must be withheld when making call by prefixing the dialed number 141.
- Staff and volunteers should ensure that all communications are transparent and open to scrutiny. They should be circumspect in their communities with pupils in order to avoid any possible misinterpretation of their motives or any behaviour which could possibly be construed as 'grooming' in context of sexual offending.
- E-mail or text communication between members of staff and volunteers and a pupil should only take place within the agreed protocols and for email within the confines of the Acceptable Use Policy.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will easily be recognized and should be openly acknowledged with the Headteacher where there may be implications for the adult and the position within the school setting

Reporting/Posting

Posting on behalf of the school

Staff members are not permitted to post on behalf of school without specific permission, which will apply to specific sites

Social Networking Good Practice

Staff and volunteers must understand who is allowed to view the content of their page of any sites they use and how to restrict access to certain groups of people.

- On FACEBOOK, they should understand whether the posts they make are public (which means that anyone can see them), visible to Friends (which means only people on their friends list can see them) or visible to friends of friends (which means posts are visible to all their friends of their friends which could be hundreds even thousands of people)
- On TWITTER and LINKEDIN, all posts, unless they are direct messages to another user, are visible to everyone (the whole world)
- If you are unsure of who can see your posts on other sites, you could always assume that the information is publically available to all and could be found by people doing a search on Google, for example.

Before posting, staff and volunteers should ask themselves the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the setting of other, or people can copy and paste information into other public places.
2. Do you want the post to be forever? Once you have posted something, it is almost impossible to delete it again from the internet, even if you delete it from the sites. There are sites that archives all Twitter posts, for example, so even if you delete a post it can still be found.
3. What information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online , maybe used inappropriately by others.
4. Could the information out you or others in danger? What you post could tell others that your house is empty or that pupils in your class are in a school trip, which could have implications for a looked after child.
5. Are you violating any laws? The information could be breach of copyright, or specific legislation relating to privacy of vulnerable groups, for example. What you post could be illegal in other countries, which could have serious implications if you were to visit there, Are you making claims that could be taken as facts when they are not? This could lead to you being accused of slander.
6. Is your message clear? Could you unintentionally break cultural norms or putting out something unintentionally offensive? Is it clear whether or not you are posting in an official capacity?
7. Could the actions of your social networking friends reflect on you? Could your friends or friends 'tag' you in a photograph or link you inappropriate activities through their own posts? Choose your friends carefully.

Access to inappropriate Images

Although this is covered in the Acceptable Use Policy, there is an overlap with social networking, so these principles are re-stated for the purpose of clarity:

- There are no circumstances that justify adults possessing images of children. Staff and volunteers who access and/or possess links to such material or websites will be viewed as a significant and potential threat to children. This will lead to criminal

investigations and disciplinary action. Where indecent images of children are found, the Headteacher will be informed immediately.

- Adults must not use equipment belonging to school to access any adult pornography; neither should personal equipment containing images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
- Adults should ensure that all pupils are not exposed to any appropriate images or web links. The school endeavours to ensure that internet equipment used by pupils has appropriate controls with regards access. E.g. personal password should be kept confidential. Any potential issues identified must be reported to the ICT lead or ICT technician, if this is a significant issue report to the Headteacher.
- Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, high level advice should be sought before any investigation is conducted.
- Staff and volunteers should be aware that they could be drawn into an investigation of child pornography or obscene images if they are linked to someone under investigation through social media networking sites. They should inform the Headteacher immediately if they are contacted by the police or other investigators.

Cyberbullying

Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control them.'

If cyberbullying does take place, employees should keep records of abuse, text, emails, websites or instant message and should not delete text or emails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Employees are encouraged to report any and all incidents of cyberbully to their line manage or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. Employees may wish to seek the support of their union or professional association representatives.