St John's RC Primary School

Social Media Policy
2017

Social Media Policy

Introduction

This policy applies to all staff employed at St John's RC Primary School. In addition the principles pertaining to the policy apply to workers and volunteers who also have a personal responsibility for their online behaviour and ensuring their use of social networking media takes place within appropriate boundaries and does not bring the individual, or the School, into disrepute.
Computing and the Internet provide a number of benefits, from rediscovering old school friends on Facebook to keeping up with other people's daily lives on Twitter or helping to maintain open access online encyclopedias, such as Wikipedia.

Even if a person's social media activities take place completely outside of work, as their personal activities should, what they say can have an influence on their ability to conduct their job responsibilities, their work colleagues' abilities to do their jobs, and the Schools interests and reputation.

Accordingly, employees are expected to behave appropriately when on the Internet, and in ways that are consistent with the School's values and policies. This policy sets out the principles which employees of the School are expected to follow when using the Internet and gives interpretations for current forms of interactivity. It applies to blogs, to micro blogs like Twitter and to other personal web space. The Internet is a fast moving technology and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The School aims to regularly review all of its recommended policies and procedures to ensure there are no negative equality impacts on staff based on their age, disability, gender, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief and sexual orientation as outlined in the Equality Act 2010. Consultation with our staff is an important part of how we achieve this.

Use of Schools IT equipment

1. All employees of the School who use the School computers should have read, understood and signed the School's ICT Acceptable Use Policy.
2. Employees must protect the security of the Schools IT network and information at all times.
3. Do not install any application without prior permission.
4. Employees should not open any emails from people they don't know and trust, particularly if they have attachments. Such emails should not be forwarded within the School unless the employee knows that they are virus free.
5. Remember online activity can be traced back to the School and the user. Do not do anything online that breaches the Schools Computing Policies and Procedures.
6. Do not reveal any details of the School's Computing systems and services, including what software is used for email, Internet access and virus protection, to minimise the risk of malicious attack.

What is Social Media?

Facebook, Twitter, blogs, YouTube, Wikipedia and networking sites such as LinkedIn or IDeA Communities of Practice are all examples of social media. The term covers anything on the Internet where content is created and adapted by the people who use the site and which allows two-way conversations.

Schools are increasingly looking to social media to engage with their audiences. People expect to 'talk back' when organisations communicate with them and they expect that those agencies will in turn respond and do so in appropriate language.

New media enables that kind of interaction to happen in a more efficient manner than, for instance, arranging formal meetings.

Audiences are also becoming fragmented and diverse, the old ways of communicating, where budgets were invested into a newsletter or another form of mass communication that contains one standard message and assumes this will be effective for everyone is increasingly losing impact. Information needs to be provided in a variety of formats so each target audience can choose how to access it. Photographs can tell a thousand words and videos are very accessible for a wide audience.

Benefits of using Social Media

Used carefully social media can bring people together over common interests, and can be useful for consulting people, obtaining feedback and publishing information that other media may ignore. However, it is important to treat social media with respect. Always remember any information or comments published on any site (internal or external):

- may stay public for a long time
- can be republished on other websites
- can be copied, used and amended by others
- could be changed to misrepresent what was said
- can attract comments and interest from other people/the media

Always be aware of the standards, conditions of use and guidelines for posting laid down by the owner of any site or network and ensure compliance with them.

Using Social Media

This policy applies to all employees of the School participating in any on-line social media (whether listed here or not), whether privately or as part of their role with the School and sets out the standards of behaviour the School expects of all of its employees.

The intention of this policy is not to stop employees of the School from conducting legitimate activities on the Internet, but serves to identify those areas in which issues/conflicts can arise.

To this end, employees:

- should not engage in activities on the Internet that might bring the School into disrepute;
- should not conduct themselves in a way that is detrimental to the School's reputation;
- should not use the Internet in any way to send or post abusive, offensive, hateful or defamatory messages;
- should act in a transparent manner when altering online sources of information;
- should not post information that could constitute a breach of copyright or data protection legislation;
- should only use their work email addresses for official School business;
- should obtain approval from their line manager in advance for any online activities associated with work for the School;
- should not use the School's IT systems for party political purposes or for the promotion of personal interests; and
- should take care not to facilitate interaction on these websites that could cause damage to working relationships between employees of the School, the School and the wider community.

Personal use of the Internet at work

The School has developed Computing systems to assist employees with their work. The School does, however, recognise that there are times when employees may want to use the Computing systems for non-work related purposes, and in recognising this need the School permits employees to use the IT systems for responsible personal use.

Employees will only be able to access the internet on personal devices in staff zones where the children are not permitted. Staff can use their phones during personal break time and lunch time when children are not present. The only time they are permitted to use their phones during the day is if there is an emergency. Employees must not allow personal use of the Computing systems to interfere with their day to day duties or the duties of others.

If, within the above parameters, employees choose to use the School's Computing systems to access social networking sites and/or other online forums, blogs etc. they must do so in a responsible and appropriate manner. There is no unconditional right for an employee to access such sites and the School reserves the right to restrict access to the Internet (or certain websites) for particular employees if there is cause for concern over their use.

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private.

Online contact with children and young people

From a safeguarding perspective, there is a widely held concern that social networking may increase the potential for sexual exploitation of children and young people, or provide opportunities for "grooming" to take place. It is also possible that those who work with children and young people may be at risk from false allegations being made against them. It is therefore vital that employees use social media responsibly and, with these concerns in mind, take appropriate steps to protect themselves from allegations, maintain appropriate boundaries, exercise appropriate judgment and avoid any contact that may lead to their intent and motivations for any such dialogue to be questioned.

Employees in a School have a duty to safeguard children and young people, and it is therefore inappropriate for employees to communicate via social networking sites with pupils and/or ex pupils.

Personal devices belonging to employees, such as mobile phones or laptops, should never be used by any pupils or children within the care and trust of the School.

Specifically in respect of social media, employees of the School should not share personal information with children/young people and must not become Facebook friends with any child or young person to whom they have acted in a position of trust. It would be recommended that the same approach is taken with parents. Extreme care must be exercised when using Twitter or other similar sites to establish the identity of "followers" and when using online chat rooms, as it may be difficult to ascertain to whom you may be chatting. Should a young person attempt to contact an employee of the School via social networking, this should be reported to their manager immediately.

Any inappropriate conduct in relation to online communication with children and young people will be taken extremely seriously and investigated in line with safeguarding and/ or the School's Disciplinary Procedure.

Online bullying and harassment

Social media does have potential dangers and drawbacks. In society in general, adults, as well as children have found themselves the target of online abuse, bullying and harassment (cyber-bullying), including name calling/ malicious comments, exclusion, intimidation, spreading of rumors, or bombarding with unwanted messages.

Bullying or harassment of any kind, including using online channels is totally unacceptable and will not be tolerated. Cyber-bullying can have a significant impact upon the health, wellbeing and confidence of those targeted, and because technology is accessible 24/7, it can impact upon an individual's private life.

Support is available for any employees who feel they have been bullied or harassed via social networking sites through their Trade Union representative, as well as in School. In the first instance, staff should refer any cyber bullying concerns to the Head teacher, who will be able to provide information and guidance.

All complaints regarding bullying or harassment will be treated extremely seriously.

Monitoring of online access at work

Employees should be aware that, in order to protect its legitimate business interests and its Computing systems, the School reserves the right to monitor internet use in accordance with the provisions set down in the Schools Computing Policies and Procedures.

Inappropriate Posting

If an employee is found to have posted inappropriate material in any format on the Internet, they will be required to assist in any way to ensure such material is removed without delay.

Staff should remember that colleagues and parents may see their online information (e.g. Facebook). Whether they identify themselves as an employee of the School or not, staff are encouraged to think carefully about how much personal information they want to make public and make sure their profile and the information they post reflects how they want themselves to be seen, both personally and professionally.

Disciplinary Implications

If the School finds that an employees' internet use is not in accordance with this policy, access to the Internet through the school's Computing systems may be withdrawn.

Employees must be aware that if they do not adhere to this policy, disciplinary action may be taken in line with the School's Disciplinary Procedure. If deemed sufficiently serious, this could result in dismissal.

Security and online identity theft

Employees are reminded to be Computing security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites and online forums allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which may form the basis of security questions and passwords.

Employees must take care when posting such information, in order that it does not allow a breach of Computing security within the School, or raise the possibility of the employee's online identity being stolen.

Employees are advised to think carefully about who they give out personal details to, like home addresses, phone numbers, financial information or full date of birth, to prevent online identity theft.

In addition, employees should:

- ensure no information is made available that could provide a person with unauthorised access to the School and/or any confidential information belonging to the School, employees, pupils and/or members of the public; and
- refrain from recording any confidential information regarding the School, employees, pupils and/or members of the public on any social networking website

Employees should note that if they are found to have posted confidential material regarding the School in any format online, they are required to assist in any way to ensure such material is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

Compliance with the law

Employees are required to stay within the law at all times when communicating online. They need to be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line, just as they do in any other form of the media.

Libel - If a person publishes an untrue statement about another person, which is damaging to their reputation, the latter may take a libel action against them. This will also apply if that person allows someone else to publish something libellous on their website if they know about it and don't take prompt action to remove it. A successful libel claim against a person will result in an award of damages against them.

Copyright - Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc.), which without permission is likely to breach copyright laws. Employees should avoid publishing anything they are unsure about, or seek permission in advance. Breach of copyright may result in an award of damages against that person.

Data Protection – Employees should not publish the personal data of individuals unless they have their express written permission.

Obscene material - It goes without saying that employees should avoid publishing anything that people would consider obscene. Publication of obscene material is a criminal offence. In addition, a person who posts grossly offensive or indecent material may be found to be guilty of an offence under the Communications Act 2003.

Privacy and decency when online

Employees must at all times remember their responsibilities to the School, parents, pupils and colleagues, and never give out details of or divulge dealings with colleagues, parents or pupils without their explicit consent. Employees should check with their manager if they are not sure what is and is not confidential.

Employees must not use slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace. That could bring the School into disrepute, break the law and leave the employee open to prosecution and/or disciplinary action.

Employees are encouraged to be themselves, but to be considerate about other people's views, especially around contentious topics.

Employees are encouraged to be credible, accurate, fair and thorough and ensure they are doing the right thing.

Employees are encouraged to share useful information that they gain from using social media with others, where appropriate.

Communicating online on behalf of the School

Employees should not comment on behalf of the School (disclose information, publish information, make commitments or engage in activities on behalf of the School), unless they are specifically authorised to do so by the Head teacher and/or the Chair of Governors. If not specifically authorised to do so, they should speak to the Head teacher before taking any action. Remember employees are personally liable for what they publish online.

This policy was ratified by the Governing Body in **2017.**
The policy will be reviewed again in **September 2018.**