Broomwood Primary School Social Networking Policy Draft

Introduction

This policy outlines the way in which the use of social networking is acceptable by staff members within our school. This policy applies to all staff employed at the School. In addition, the principles pertaining to the policy apply to workers and volunteers who also have a personal responsibility for their online behaviourand ensuring their use of social networking media takes place within appropriate boundaries and does not bring the individual, or the School, into disrepute. 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.

Rationale

IT and the Internet provide a number of benefits, from rediscovering old school friends on Facebook tokeeping up with other people's daily lives on Twitter or helping to maintain open access online encyclopaedias, 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 workcolleagues' 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 Internetis a fast moving technology and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

Use of Schools IT equipment

- All employees of the School who use the School computers should have read, understood and signedthe 'Acceptable Use Policy': Staff agreement form (Appendix A).
- Employees must protect the security of the Schools IT network and information at all times.
- Do not install any application without prior permission.
- Employees should not open any emails from people they don't know and trust, particularly if theyhave attachments. Such emails should not be forwarded within the School unless the employee knows that they are virus free.
- Remember online activity can be traced back to the School and the user. Do not do anything onlinethat breaches the Schools IT Policies and Procedures.
- Do not reveal any details of the School's IT systems and services, including what software is used for email, internet access and virus protection, to minimise the risk of malicious attack.
- If employees use secure systems, such as GovConnect email or to process financial transactions, they should never log onto social networking sites while connected to those systems. If they haveused a social

networking site, they should restart their computer before logging onto the secure system to clear any information in the computer's memory cache.

Social Media

What is social media?

Facebook, Twitter, blogs, YouTube, Wikipedia and networking sites such as LinkedIn are all examples of social media. The term covers anything on the internet where content is created and adapted by the peoplewho 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 doso in appropriate language. Some classes in our school have had Facebook pages and this is fine (at the discretion of the headteacher), as long as it is monitored correctly.

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 andassumes this will be effective for everybody, 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, itis important to treat social media with respect. Always remember any information or comments publishedon 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 ofany site or network and ensure compliance with them.

Using Social Media

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

Employees:

- should not engage in activities on the Internet which 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 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 protectionlegislation;
- 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 withwork for the School;
- should not use the School's IT systems for party political purposes or for the promotion ofpersonal interests;
- 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.

Blogging

- If an employee already has or plans to have a personal blog or website which shows in any way in that they work at the School, they must tell their Headteacher. They should include a simple andvisible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of XXX School"
- If an employee thinks that something on their blog or website may cause a conflict of interest, orthey have concerns about impartiality or confidentiality, they should speak to their Headteacher. If in any doubt, employees should not talk about what they do at work.
- If someone offers to pay an employee for blogging, this could cause a conflict of interest and theHeadteacher must be consulted.

Social networking & online discussions

- Employees should use their best judgment, remembering that there are always consequences towhat is published.
- Employees should not use the Schools email account or their email or work number in on-line discussions unless they have been authorised to speak for the School.
- It is not a good idea to invite parents to become friends on social networking sites. There may be aconflict of interest, security and privacy issues.

Wikis

- Employees should use their best judgment, remembering that there are always consequences towhat is published.
- Employees should not use the Schools email account or their email or work number in on-line discussions unless they have been authorised to speak for the School.
- Make sure any wiki entries, articles or comments are neutral in tone, factual and truthful.
- Never post rude or offensive comments on any online encyclopaedias.
- Before editing an online encyclopaedia entry about the School, or any entry which might cause a conflict of interest, or adding links, check the house rules of the site. Permission may be requiredfrom the relevant wiki editor and the Headteacher.
- If employees edit online encyclopaedias whilst using a work computer, the source of the correctionmay be recorded as a School IP address. That means it may look as if the School itself has made the changes. If this is correcting an error about the School, that's fine – it is important to be openabout any actions. In other circumstances employees need to exercise caution that they do not bring the School into disrepute through this. If in any doubt, ask the Headteacher before taking action.

- It is important to respond to legitimate criticism with facts, but speak to the Headteacher for advice before responding; a poor response could make matters worse. Never remove criticism ofthe School or derogatory or offensive comments. Report them to the Headteacher for them to take action.

Media Sharing (photos, videos, presentations)

- Make sure all video and media is safe to share, does not contain any confidential or derogatory information, and is not protected by any copyright, or intellectual property rights.
- If the content is official School content then it must be labelled and tagged as such.
- Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: "This ismy personal work and does not necessarily reflect the views of XXX School."

Personal use of the internet at work

The School uses a range of computing systems to assist employees with their work. The School does, however, recognise that there are times when employees may want to use these systems for non-work related purposes, and in recognising this need the School permits employees to use the IT systems for responsible personal use, in an appropriate manner. However employees must not use the IT systems (oraccess the internet through personal devices e.g. smart phones) for personal use during working hours. Staff may not use the school WiFi on personal devices.

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 falseallegations 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 judgement 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 inappropriatefor 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 pupilsor 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 rumours, 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 and HR, as well as in School. In the first instance, staff

should refer any cyber bullying concerns to the Headteacher, who will be able to provide information andguidance. 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 IT systems,the School reserves the right to monitor internet use in accordance with the provisions set down in the Schools IT Policies and Procedures.

Inappropriate Posting

If an employee is found to have posted inappropriate material in any format on the internet, they will berequired 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 andthe information they post reflects how they want themselves to be seen, both personally and professionally. Profile settings should be the highest security level and for 'friends only'.

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 IT systems may be withdrawn.

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

Security and online identity theft

Employees are reminded to be IT 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 networkingwebsites 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 IT security within the School, or raise the possibility of the employee's online identity being stolen.

In addition, employees should:

- ensure no information is made available that could provide a person with unauthorised access to theSchool and/or any confidential information belonging to the School, employees, pupils and/or members of the public;
- not record any confidential information regarding the School, employees, pupils and/or members ofthe public on any social networking website

Employees should note that if they are found to have posted confidential material regarding the School inany 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 promptaction 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 theirexpress written permission.

Obscene material - It goes without saying that employees should avoid publishing anything that peoplewould 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 anoffence 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 inthe 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 Headteacher and/or the Chair of Governors. If not specifically authorised to do so, they should speak to the Headteacher before taking any action. Employees are personally liable for what they publish online.

Policy review

This policy will be reviewed and revised in line with the developments in the Primary Curriculum and the school development plan.

Reviewed March 2023 S Walker

Approved by Governing Body____________________________________
Date____

Appendix A – 'Acceptable Use Policy': Staff agreement form

Acceptable Use Policy

Acceptable Use Policy for Employees, Governors, Volunteers and Visitors In using technology for the use of communication for education and personal use, including but not limited to: IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other mobile devices and lists the responsibilities they have in ensuring any form of communication using technology that they use in their role is used appropriately and in line with GDPR rules.

The school will try to ensure that everyone has good access to IT to enhance their role and to be able to provide the relevant learning opportunities for pupils.

Employees, governors, volunteers and visitors must ensure:

· That all technology devices have password/encryption facilities installed.

· They do not disclose or share any passwords provided for their use to others and will not attempt to gain access to anyone else's passwords. Passwords will not be written down and kept where anyone else can gain access to them.

· They do not install any hardware or software on any school-owned device without the headteacher's permission

· They are using a school email address for any correspondence they send in relation to their role in the school.

· Ensure all data is kept secure and used appropriately as authorised by the headteacher.

· They ensure that any emails with attachments that contain personal or sensitive data are encrypted or are saved onto a secure shared site giving the link to where it can be accessed.

· They know where any school owned device is at all times and be responsible for ensuring it is securely stored when not in use. Laptops/mobile devices that are taken off-site must be stored out of site securely. If left in a vehicle they must not be left in view but stored in the boot and the vehicle locked.

· They do not use school technology for personal use.

· They do not use personal technology/devices for school use at any time unless with the express permission of the headteacher. The only exception to this is if the only means of calling the emergency services to an incident is by using a personal mobile phone to do so.

· They do not use/duplicate/remove or amend anyone else's documents without their prior permission.

· They do not download, copy or distribute anything that is protected by copyright.

· They maintain professional boundaries when using the internet and social media for personal use. That when posting on personal forums/social media that there is the understanding that the use of any comments or photos regardless of whether they are positive or negative can be shared with others (parents, pupils, colleagues) and this could lead to losing control of who sees them or a misinterpretation of what was written, this could then bring your professional role and workplace into disrepute.

· They do not participate in communicating with pupils outside of their role at the school when using work or personal technology/devices for the use of social media, texting, calling. It is important to ensure that a professional relationship is adhered to at all times to prevent any misinterpretation of any actions made.

· That no personal details are exchanged with pupils that would allow contact directly via personal email, telephone, address.

· They do not use school equipment to upload, download any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or anything that is inappropriate or may cause harm or distress to others.

· That the use of school equipment to access personal sites (social media).

· That personal mobile phones must not be used in schools where children are present. Mobile phones should be put away during school hours but can be used when on a break away from pupils.

· All communications with pupils must be via the school's internal network

- They report any incidents of concern regarding social media misuse to the headteacher, computing lead and if necessary behaviour lead, this includes but is not limited to illegal, inappropriate or harmful material.
- That if any work device (laptop /ipad or similar) is stolen it must be reported immediately as this is considered a breach under GDPR and will need reporting within 72 hours.
- They agree to be responsible users at all times and understand that they are responsible for their actions and misuse or failure to comply with this policy could result in disciplinary action of a verbal, written warning, suspension, and the involvement of the police in the event of illegal activity.

Employees, governors, volunteers and visitors are asked to sign and date the form below to confirm they have received a copy of the Acceptable Use Policy for Employees, Governors and Visitors and have read and agree to adhere to it.

Agreement to adhere to the Acceptable Use Policy: I confirm that I have received a copy, read and understand that I must adhere with the above policy and understand that any breach could result in disciplinary action. I will immediately report the loss of any equipment covered by this policy. I will report any incidents of concern regarding misuse of technology/software/social media to the headteacher.

Name:
Signed:
Position:
Date: