Computing/Social Networking Policy

January 2019

Contents

1	**Introduction**	**3**
2	**Principles of the policy**	**4**
3	**Safer networking practice**	**4**
4	**Communication**	**6**
5	**Inappropriate images**	**6**
6	**Cyberbullying**	**7**

Computing Social Networking and Acceptable Use Policy

Adopted by the Governing Body of:
Armitage C of E Primary School.
Date of Issue: 15.01.19
Review Date: 15.01.20

This policy should be read in conjunction with other relevant policies e.g. school Computing Policy including acceptable or unacceptable usage, Disciplinary Policy and Procedures, Equal Opportunities Policy, Codes of Conduct.

Introduction:

All staff and workers at the school need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, the school or its pupils and staff or the wider school community in the Social Media arena.
Every employee or volunteer working within the school setting is accountable for information published and must be aware that such information may be monitored by the Headteacher or their representative.
It is important to note that information available in the public domain which has the potential for harm, distress or reputational damage may lead to disciplinary action being taken.
This policy recognises that new technologies are an integral and growing part of everyday life and make an important contribution to teaching and learning opportunities. However the rapid evolution of social networking technologies requires a robust policy framework and this policy aims to:

a) Assist staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

b) Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use as outlined in this policy.

c) Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.

d) Support safer working practice including safeguarding children from the views of extreme ideologies that they may encounter online.

e) Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

f) Prevent adults abusing or misusing their position of trust.

This document applies to all staff/volunteers/students who work in the school whether paid or unpaid.

The principles that underpin this policy are:

a) All staff who work with pupils are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.

b) All staff in the school must work and be seen to work, in an open and transparent way.

c) All staff in the school must continually monitor and review their own practice in terms of the continually evolving world of social networking and ensure that they consistently follow the guidance contained in this document.

d) All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours' of others.

e) All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.

f) All users have a duty to report failings in technical safeguards, e.g. viruses, gaps in network security etc., which may become apparent when using the systems and services.

g) All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

h) All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.

Safer Social Networking Practice

This document applies to current and future social networking sites such as Facebook, Bebo, MySpace, Whatsapp, Twitter etc and all other current and emerging technologies.

a) All users must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

b) In their own interests, adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites, such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

c) All users, particularly those new to the school setting, 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 any photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.

d) Adults should never make a ‘friend’ of a pupil at the school where they are working on their social networking page, and should be extremely cautious about becoming ‘friends’ with ex-students particularly where siblings or other relatives may continue to attend the school.

e) Staff should never use or access social networking pages of pupils.

f) Confidentiality must be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, the school, the governing body, the Local Authority, their colleagues, pupils or members of the public.

g) Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making 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 another school, or the Local Authority could result in disciplinary action being taken against them.

h) Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on their professionalism.

i) Some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee of the school and particularly if you are a teacher or teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school and the profession.

j) This document does not replace or take priority over any advice contained in the school’s codes of conduct, or other policies issued around safeguarding or IT issues. It is intended to both supplement and complement any such documents.

l) The local community and friends of Armitage are encouraged to report any incidents that may be considered to be extremist or radicalised views. In particular, if these are witnessed on social media sites amongst people that may come into contact with any of our children, they should let us know immediately.

Communications and Social Contact

a) Adults should keep their personal phone numbers, work login or passwords and personal 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.

b) Adults must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.

c) Communication between pupils and adults by whatever method, must take place within clear and explicit professional boundaries.

d) Adults must not request, or respond to, any personal information from a pupil.

e) Adults must ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils in order to avoid any possible misinterpretation of their motives or any behaviour which could possibly be construed as 'grooming' in the context of sexual offending.

f) E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems must only be used in accordance with the school's policy.

g) 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 be easily recognised and should be openly acknowledged with the Headteacher where there may be implications for the adult and their position within the school setting.

h) There must be awareness on the part of those working with or in contact with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process.
This can also apply to social networking contacts made through outside interests or through the adult's own family.

i) Any concerns must be raised with the Headteacher and the schools designated E-safety Officer Martin Goulden, at the earliest opportunity.

Access to inappropriate images

a) There are no circumstances that justify adults possessing indecent images of children. Staff 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 investigation and disciplinary action. Where indecent images of children are found, the Headteacher must be informed immediately.

b) Adults must not use equipment belonging to the school to access any adult pornography; neither should personal equipment containing these 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.

c) Adults should ensure that pupils are not exposed to any inappropriate images or web links. The school endeavours to ensure that internet equipment used by pupils has the appropriate controls with regards to access, e.g. personal passwords should be kept confidential. Any potential issues identified must be reported to the Headteacher and designated E-safety Officer Martin Goulden immediately.

d) Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, advice should be sought from Management Support to Schools before any investigation is conducted.

Cyberbullying

a) 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 over them.'

b) If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. 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.

c) Employees must report any and all incidents of cyberbullying to the designated E-safety Officer Martin Goulden, 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 trade union or professional association representatives.

Links to other school policies/external sources of information
Disciplinary policy and procedures
Equal opportunity policy
Guidance for Safer Working Practice for Adults who Work with Children and Young People – available to download at:
http://www.childrenengland.org.uk/upload/Guidance%20.pdf
Cyberbullying – Supporting School Staff - available to download at:
http://old.digizen.org/cyberbullying/default.aspx
Manchester Safeguarding Children Board E-Safety – Guidelines for Minimum Standards – available to download at:
http://www.manchesterscb.org.uk/docs/Minimum_Standards_V2.1.pdf