Aylesford School

and Sixth Form College

wonder aspiration respect discipline

Social Networking Policy

Written/Updated:	June 2020
Review Date:	June 2021
Lead:	Headteacher
Via:	Standards, Personnel and Curriculum

‘from potential to reality’

Tapping Way, Warwick, Warwickshire, CV34 6XR
Tel: 01926 747100 **Fax:** 01926 494194 **Email:** office@aylesfordschool.org.uk **Web:** www.aylesfordschool.org.uk
A charitable company registered in England and Wales, company number 7848367
Headteacher: Tim Hodgson

Contents

Section 1: Introduction

1.1 Objectives

1.1.1 This document sets out Aylesford School's policy on social networking and aims to:

- 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.
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use.
- Provide a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Support safer working practice.
- Minimize the risk of misplaced or malicious allegations made against adults who work with students.
- Prevent adults abusing or misusing their position of trust.
- To support the school's legal obligations as an identified *specified authority* under Schedule 6 of the Counter Terrorism and Security Act 2015 to *"in the exercise of its functions have due regard to the need to prevent people from being drawn into terrorism."*

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognized that this policy cannot cover all eventualities. There may be times when professional judgments are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in school will always advise the headteacher of the justification for any such action already taken or proposed. In these circumstances, where appropriate, the school may seek the advice of outside agencies such as the Warwickshire Safeguarding Children Board (WSCB) or legal counsel.

1.1.3 This policy takes account of current employment legislation, and best practice guidelines in relation to social networking in addition to both the normal legal obligations of governing bodies and current statute law.

1.2 Scope

1.2.1 This document applies to all adults who work in 'Aylesford School and Sixth Form College' as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors employed by the school and volunteers.

1.2.2 The stipulations and guidance provided in this document should be followed by any adult whose work brings them into contact with pupils. References to adults should be taken to apply to all the groups (see 1.2.1) of people in schools. Reference to pupils in this document means all pupils at the school including those over the age of 18.

1.2.2 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of existing policies adopted by the school (see 3.1.1) requires the school first comply with any child protection requirements as set out in these existing policies.

1.2.3 For the purposes of this policy a pupil is defined as a current or former student less than 18 years of age.

1.2.4 Breaches of this policy may result in disciplinary action up to and including dismissal.

Status

1.3.1 This document does not replace or take priority over advice given by the school's safeguarding policy, GDPR arrangements, the school's grievance or disciplinary policies, or other policies issued around safeguarding or IT issues (email, ICT and data protection policies), but is intended to both supplement and complement any such documents.

Principles

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults in schools should work and be seen to work, in an open and transparent way.
- Adults in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice in Schools

2.1 What is social media?

2.1.1 For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook and Google+ are perhaps the most well-known examples of social media but the term also covers all other digital communication services such as blogs, location based services such as Foursquare, messaging systems, multiplayer online games, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as Vimeo, Flickr, or YouTube, mobile social communication applications such as Snapchat and micro blogging services such as Twitter or Medium. In addition, the use of telepresence software such as Zoom or Microsoft Teams also comes within the scope of this policy. However, this definition of social media is not intended to be exhaustive as technology in this area is rapidly developing with new methods of electronically assisted social interaction appearing with increasing frequency.

2.1.2 For the purpose of this document the term '*Social Media'* is not exhaustive and also applies to the use of digital communication technologies such as mobile phones, cameras, PDAs / PSPs, telepresence equipment, or other handheld devices and any other emergent forms of communication technology.

2.2 Overview and expectations

2.2.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using professional judgement and integrity about behaviour in places other than the work setting.

2.2.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the school setting who work with or have contact with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

2.2.3 Adults within the school setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

2.3 Safer online behaviour

2.3.1 Managing personal information effectively makes it far less likely that information will be misused.

2.3.2 In their own interests, adults within school settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and 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.

2.3.3 All adults, 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 the school if they are published outside of the site.

2.3.4 Adults should never make a ‘friend’ of a pupil at the school where they are working on their social networking page, and should be cautious about becoming ‘friends’ with ex-students where sibling continue to attend the school.

2.3.5 Staff should never use or access social networking pages of pupils and should never accept an invitation to invite a pupil to become a ‘friend’.

2.3.6 Confidentiality needs to 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, their employer, their colleagues, pupils or members of the public.

2.3.7 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. In particular, thoughtless, callous or intentionally damaging comments communicated through social media can be viewed as either slanderous or libellous with the attendant risk of serious consequences for those deemed to have broken the law. Making personal allegations, intentionally damaging inferences or threats on social networking sites (even in their own time and in their own homes) about other employees, pupils or any other individuals connected with the school, or indeed another school, could also result in formal action being taken against them by their employer.

2.3.8 Adults are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

2.3.9 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, its staff or governing body into disrepute or could reflect negatively on their professionalism.

2.3.10 Many social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of the school and particularly if you are a teacher/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, the profession or the governing body.

2.4 Protection of personal information

Adults working at Aylesford School should:

2.4.1 Never share their work log-ins or passwords with other people.

2.4.2 Keep their personal phone numbers private.

2.4.3 Not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used.

2.4.4 Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.

2.4.5 Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

2.4.6 Staff employed by the school must never knowingly allow or instigate the communication or publication on social media of personal or sensitive data acquired through their professional duties at the school. Such actions would constitute a serious breach of both this policy and an employee's obligations to ensure the security of personal information under the current GDPR regulations.

2.5 Communication between pupils / adults working in school

2.5.1 Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries.

2.5.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, telepresence software, websites and blogs.

2.5.3 The school normally provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.

2.5.4 Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

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

2.5.6 Adults should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

2.5.7 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 should only be used in accordance with the school's policy.

2.6 Social contact

2.6.1 Adults should not establish or seek to establish social contact via social media or other communication technologies with pupils.

2.6.2 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 recognized and should be openly acknowledged where there may be implications for the adult and their position within the school setting.

2.6.3 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.

2.7 Access to inappropriate images, websites, social media apps and internet use

2.7.1 There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal and malpractice in this area would lead to prosecution and termination of employment if proven.

2.7.2 Adults should not use equipment belonging to their school/service to access any adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. Any infringements in this matter would raise serious concerns about the suitability of the adult involved to continue to work with children.

2.7.3 Adults should take all reasonable precautions to ensure that pupils are not exposed to any inappropriate images or web links. The School needs to ensure that internet equipment used by pupils has reasonable and appropriate controls in place and access to personal passwords should be kept confidential.

2.7.4 Where indecent images of children are found, the police and the designated school 'Child Protection' officer should be immediately informed. The school should refer to their existing grievance or disciplinary policies and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

2.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about a member of staff, the head teacher and school designated 'Child protection Officer' should be informed and advice sought. Schools should refer to their existing grievance or disciplinary policies and staff should not attempt to investigate or evaluate the material themselves until advice or direction is received.

2.7.6 The Counter Terrorism and Security Act 2015 places a specific responsibility upon adults employed by the school to take all reasonable steps to ensure that students are neither exposed to or can gain access to online material of any nature that **advocates**, (outside the realm of accepted fictional media or approved educational purposes), an act of terrorism or

(a) serious violence against a person,

(b) serious damage to property,

(c) endangering a person's life, other than that of the person committing the action,

(d) creating a serious risk to the health or safety of the public or a section of the public

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

2.7.7 No adult employed by the school should use social or communications technology to engage in activities (outside of the realm of accepted fictional media or for approved educational purposes) that **advocate or involve**.

(a) serious violence against a person,

(b) serious damage to property,

(c) endangering a person's life, other than that of the person committing the action,

(d) creating a serious risk to the health or safety of the public or a section of the public

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

2.8 Cyber-bullying

2.8.1 Cyber-bullying 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.’

2.8.2 Prevention activities are vital to ensuring that adults are protected from the potential threat of cyber-bullying. All adults are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If cyber-bullying 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.

2.8.4 Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.

2.8.5 Adults are encouraged to report all incidents of cyber-bullying to their line manager 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.

Section 3: Review of policy

3.1.1 Due to the ever changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.