Diocese of Salisbury
Academy Trust

SOCIAL MEDIA AND NETWORKING POLICY

for employees in
Diocese of Salisbury Academy Trust

This model policy will apply to both teaching and non-teaching staff

For adoption and implementation from

Approved

Amended after HR circulation

This policy is a mandatory policy for all DSAT Academies and must be implemented with no amendments.

Contents

1. Introduction

1.1 This policy sets out the Diocese of Salisbury Academy Trust (DSAT)'s policy on social networking for <Academy>. It applies to all permanent, temporary and casual employees at the Academy – at all times when <Academy> employees are making use of social media sites. This may be at home or at work and whether they are using Academy equipment or their own device.

1.2 New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for Academy staff in many ways. It allows for great freedom in how people communicate and express themselves. This document sets out DSAT policy on social networking and aims to assist DSAT and <Academy> staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice

1.3 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements 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 <Academy> will always advise their Principal/Headteacher of the justification for any such action already taken or proposed. Principals/Headteachers will in turn seek advice from the DSAT HR team where appropriate.

2. Scope

2.1 This policy should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in DSAT Academies. Reference to pupils means all pupils at DSAT Academies including those over the age of 18.

3. Principles

3.1 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.

3.2 Staff in <Academy> should work and be seen to work, in an open and transparent way.

3.3 Staff in <Academy> 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.

4. Safer Social Media Practice in Academies

4.1 **What is Social Media?**

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 Twitter are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

4.1.1 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

4.2 **Overview and Expectations**

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 Academy's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

4.2.1 The guidance contained in this policy is an attempt to identify what behaviours are expected of <Academy> staff who work 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.

4.2.2 <Academy> staff 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.

4.3 **Safer Online Behaviour**

Managing personal information effectively makes it far less likely that information will be misused. In their own interests, staff 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 Academy environment. It also reduces the potential for identity theft by third parties.

4.3.1 All staff, particularly new staff, should review their social networking sites when they join the Academy to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and <Academy> if they are published outside of the site.

4.3.2 Staff should never 'friend' a pupil at <Academy> where they are working onto their social networking site.

4.3.3 Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

4.3.4 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.

4.3.5 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 <Academy>, or another DSAT Academy, or DSAT could result in formal action being taken against them.

4.4. **Protection of Personal Information**

Staff should ensure that they do not use <Academy> ICT equipment for personal use, e.g. camera or computers.

4.4.1 Staff should keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.

4.4.2 Staff should never share their work log-ins or passwords with other people

4.4.3 Staff should not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically, the <Academy> e-mail address should be used.

4.4.4 Staff should keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on Academy premises.

4.4.5 Staff are advised to 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.

4.5 **Communication between Pupils/Academy Staff**
Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

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

4.5.2 It is the expectation that <Academy> should provide a work mobile and e-mail address for communication between staff and pupils. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.

4.5.3 Staff 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.

4.5.4 Staff 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.

4.5.5 Staff 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.

4.5.6 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 <Academy's> policy.

4.6 **Social Contact**
Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

4.6.1 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 openly acknowledged.

4.6.2 There must be awareness on the part of those working 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 staff member's own family.

4.7 **Access to Inappropriate Images and Internet Usage**
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. This will lead to criminal investigation and the individual being barred from working with children, if proven.

4.7.1 Staff should not use equipment belonging to their Academy/service to access any 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.

4.7.2 Adults should ensure that pupils are not exposed to any inappropriate images or web links. <Academy> staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

4.7.3 Where indecent images of children are found by staff, the police and local authority designated officer (LADO) should be immediately informed. Academies should refer to the dealing with allegations of abuse against staff and volunteers policy 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.

4.7.4 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either DSAT HR or the LADO should be informed and advice sought. Academies should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

4.8 **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 over them.'

4.8.1 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.

4.8.2 Staff are encouraged to report all incidents of cyberbullying to their line manager or the Principal/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.

5. Staff Roles and Responsibilities

5.1 Teacher/Employee Responsibilities

5.1.1 To carefully consider, before posting content on social media sites, whether it will bring <Academy> into disrepute, breach confidentiality or copyright or be considered offensive, defamatory, discriminatory, bullying or is potential harassment.
If you are unsure of whether it is appropriate to post certain content on a social media site advice can be sought from the Principal/Headteacher.

5.2 Principal/Headteacher Responsibilities

5.2.1 The Principal/Headteacher is not expected to monitor personal use of social media by staff. However if a matter relating to inappropriate use of social media is brought to their attention, they are responsible for looking into the matter in line with the relevant Academy policy.

6. How the Academy Protects Itself

6.1 *Amend the following paragraphs to reflect specific monitoring activity*
<Academy> will monitor social media websites in the same way as it monitors other media channels (e.g. local press etc.) for relevant content about the Academy.

<Academy> will not routinely monitor the webpages that an employee can access from their Academy laptop, however full logs are retained and can be accessed as part of a genuine investigation.

<Academy> does not monitor employee's personal social media pages without reason. However, as with any allegation of misconduct, the Academy will investigate where breaches of this policy are brought to its attention by any means (e.g. via members of the public, employees, pupils/students).

7. Examples of Social Media Sites

Social networking sites (e.g. Facebook)	Users create personal profiles, add other users as friends and exchange messages, including automatic notifications when they update their own profile. Additionally, users may join common-interest user groups, organised by common characteristics.
Blogging and micro-blogging sites (e.g. Twitter)	A blog is a type of website or part of a website usually maintained by an individual with regular entries of commentary and descriptions of events (blogging). A micro-blog is simply smaller in size.
Professional networking sites (e.g. LinkedIn)	Business-related social networking sites mainly used for professional networking. Users maintain a list of contact details of people with whom they have some level of relationship, called connections. This list of connections can then be used to build up a contact network, follow different companies and find jobs, people and business opportunities.
Online communities (e.g. MySpace)	An online community of users' personal profiles. These typically include photographs, information about personal interests and blogs. Users send one another messages and socialise within the community.
Video sharing websites (e.g. YouTube)	A website on which users can upload, share, and view videos. A wide variety of user-generated video content is displayed, including film and TV clips as well as amateur content such as video blogging. Most videos enable users to leave and exchange comments.
Collaborative web projects (e.g. Wikipedia)	Web-based projects where articles are written collaboratively by volunteers around the world, and almost all articles are freely editable by any visitor.