SEVERN ACADEMIES
EDUCATIONAL TRUST

SEVERN ACADEMIES EDUCATIONAL TRUST

Social Media Policy

September 2018

office@saet.co.uk

SEVERN ACADEMIES
EDUCATIONAL TRUST

Social Media Policy

Contents: **Page No.**

1. Introduction

This policy should be read in conjunction with other relevant policies, e.g. each school's Acceptable Use Policy, Disciplinary Policy and Procedures, Code of Conduct.

All employees within the Trust need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, their organisation and students within and the wider school community in the local area.

Every employee or volunteer is accountable for information published when working within the school setting and must be aware such information may be monitored by the Headteacher/Principal/CEO 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.

2. What is Social Networking and Social Media?

Social Networking and Social Media are communication tools based on websites or networks which allow you to share information or other material about yourself and your interests with groups of other people.

These groups of people could be:

- People who are known to you (friends or colleagues)
- People you don't know but who share common interests (such as within teaching, within the local area, etc.)
- Anyone who could find your comments through search engines.

Some examples of Social Networking and Social Media sites and services include:

- Facebook
- Twitter
- YouTube
- Instagram
- Blackberry Messenger (BBM)
- LinkedIn
- Mailing lists

3. What Social Media activity does this policy cover?

This policy is mainly concerned about two types of Social Media activity:

- Your own personal activity, which your friends or contacts could view
- Activity carried out in the name of an individual school or the Trust that represents or appears to represent the official view of both

This policy is not about stopping you using or accessing Social Media but aims to ensure that your use of Social Media does not harm the interests of the children and young people we support, or damages the reputation of our schools or the Trust, including all employees within. Adherence with the guidelines in this policy will help protect you against posting things that you might regret or may harm you later, or which might impact negatively on schools in the Trust or the Trust itself.

Aim of this policy

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:

- Assist employees 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.
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.
- Support safer working practice.
- Minimise the risk of misplaced or malicious allegations made against employees/volunteers who work with students.
- Prevent employees/volunteers abusing or misusing their position of trust.

This policy applies to all employees within the Trust whether paid or unpaid. This includes members of each Local Governing Body and Directors and Members within the Trust.

Principles

The principles that underpin this policy are:

- Employees/volunteers who work with students 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.
- Employees/volunteers within each school must work and be seen to work, in an open and transparent way.
- Employees/volunteers within each school must continually monitor and review their own practice in terms of the continually evolving world of Social Networking and ensure that they have consistently followed the guidance contained within this policy.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in social media that they have later regretted, because that information has harmed or put at risk themselves or others. This includes:

- Accidentally posting personal or embarrassing information about themselves or others in a public forum or beyond the group the information was originally intended for.
- Sharing information about yourself or others with people you don’t know that could be used by someone to commit fraud or misrepresent the views of yourself or others (identity theft).
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and employees/volunteers that you work with.
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.

This has led to people facing disciplinary action, being prosecuted and even imprisoned.

This policy and procedure will help to make sure that your use of Social Networking sites and Social Media is safe.

Safer Social Networking Practice

This policy applies to current Social Networking sites such as Facebook, Twitter, LinkedIn, Instagram and all other current and emerging technologies.

- Things you must not do, because they are either; illegal, contrary to regulations, contrary to school policies.
- Things you should do to avoid risk to yourself or others.
- Good Practice things you should do to reduce the risk that information you put on Social Networking sites or Media cannot later be used against you.

All employees and volunteers 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.

Social Networking 'Don'ts'

- Do not make comments about the Trust or any school, or claim to represent the views of the Trust or each school.
- Do not respond to any comments made by others that may be brought to their attention on social media. Such occasions must be reported to the Headteacher/Principal for advice.
- Care should be taken to ensure that social media profiles are not associated with individuals or organisations that the Trust or schools within the Trust may consider to be in conflict with their values and principles.
- Never make a 'friend' (or equivalent) of a current student at any school within the Trust on Social Networking pages.
- Never use or access social networking pages of students.
- Do not request, or respond to, any personal information from a student, i.e. messaging them privately.
- Never post confidential information about our schools, or any person connected with them.
- Do not make allegations on Social Networking sites (even in your own time and in your own home) about other employees or students within the Trust, another school, or any other organisation and the people connected with them. Doing so may result in disciplinary action being taken. If an employee or volunteer has concerns about practices within the School/Trust they must act accordingly with the Whistleblowing Policy.
- E-mail communications between an employee/volunteer and a student must not take place outside of agreed protocols (the Acceptable Use Policy).
- Care must be taken in discussing professional matters with fellow colleagues on social media to ensure that the Trust or schools are not brought into disrepute. For example, to be aware of the restrictions on sharing / discussing examination board assessment material and copyright resources.

Social Networking 'Dos'

- All employees/volunteers, particularly those new to the school setting, should review their social networking sites when they join any of our Trust schools 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 Trust or each school if they were to be published outside of the site.
- In their own interests, employees/volunteers within school settings need to be aware of the dangers of putting their personal information onto social networking sites such as addresses, contact details. This will avoid the potential for students or their families having access to employees details outside of the school environment. It also reduces the potential for identity theft by third parties.
- Some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee or volunteer 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. If it is a work-based site where you are required to provide this information, you must obtain the permission of the Headteacher/Principal, unless the site is on the list of approved sites for each school.
- Keep personal phone numbers, work login or passwords and all personal email addresses secure and private. Where there is a need to contact students or parents the school email address and/or telephone should be used. If, with permission, telephone calls are made from a personal phone (landline or mobile phone) the telephone number the call is being made from must be withheld when making calls by prefixing the dialled number with 141.
- Ensure that all communications are transparent and open to scrutiny. Staff should also be circumspect in their communications with students in order to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
- Electronic communications between an employee or volunteer and a student should only take place within agreed protocols and for email within the confines of the Acceptable Use Policy.
- There will be occasions when there are social contacts between students and staff, where for example the parent and employee are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Headteacher/Principal where there may be implications for the adult and their position within the school setting.

Posting on behalf of each school/the Trust

Staff members are not permitted to post on behalf of each school/the Trust without specific permission, which will apply to specific sites.

For example, the Headteacher/Principal may give permission for staff to post in relation to specific discussion groups related to SEN. In such cases, the Headteacher/Principal will make it clear the capacity in which the person may post and the scope and subject of their postings. The Headteacher/Principal/CEO will keep a central log of those who may post on behalf of each school and/or the Trust.

Social Networking Good Practice

Employees and volunteers 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.

- On Facebook, employees should understand whether the posts they make are Public (which means that anyone can see them), visible to Friends (which means that only people on their Friends list can see them) or visible to Friends of Friends, which means that the posts are visible to all of the friends of their friends, which could be many hundreds or even thousands of people.
- On Twitter or LinkedIn, all posts, unless they are direct messages to another user, are visible to everyone (the whole world). Twitter has a setting in the privacy option and if this is selected then only the followers of the account can see the tweets, when the account is searched for this cannot be seen.
- If you are unsure of who can see the posts on other sites, you should always assume that the information is publically available to all and could be found by people doing a search on Google, for example.

Before posting, employees and volunteers should ask themselves the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the settings of others, or people can copy and paste the information into other, public, places.
2. Do you want the post to be seen forever? Once you have posted something, it is almost impossible to delete it again from the internet, even if you delete it from the site. There are sites that archive all Twitter posts, for example, so even if you delete a post from Twitter, it can still be found.
3. What if the information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online, may be used inappropriately by others.
4. Could the information put you or others in danger? What you post could tell others information about LAC or SEN needs and their vulnerability. General Data Protection Regulations state that personal data should be processed in an appropriate manner to maintain security and processed lawfully and fairly, limited to what is necessary.
5. Are you violating any laws? The information could breach copyright, or specific legislation relating to privacy of vulnerable groups, for example. What you post could be illegal in other countries, which could have serious implications if you were to later visit there. Are you making claims that you could be taken as facts when they are not? This could lead to you being accused of slander.
6. Is your message clear? Could you unintentionally be breaking cultural norms or putting out something unintentionally offensive. Is it clear whether or not you are posting in an official capacity?
7. Could the actions of your social networking friends reflect on you? Could your friends or friends of friends 'tag' you in photographs or link you to inappropriate activities through their own posts? Choose your friends carefully.

Access to inappropriate images

Although this is covered under the Acceptable Use Policy, there is an overlap with Social Networking, so these principles are re-stated here for the purpose of clarity:

- There are no circumstances that justify employees/volunteers possessing indecent images of children/students. Employees/volunteers 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/students are found, the Headteacher/Principal and CEO must be informed immediately.
- Employees/volunteers 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 employee/volunteer to continue to work with children/students.
- Employees/volunteers should ensure that students/children are not exposed to any inappropriate images or web links. The Trust and each school within endeavours to ensure that internet equipment used by students has the appropriate controls with regards to access, e.g. potential password should be kept confidential. Any potential issues identified must be reported to the Headteacher/Principal/CEO immediately.
- Where other unsuitable material is found, which may not be illegal but which could o does raise concerns about a member of staff, high level advice should be sought before any investigation is conducted.
- Employees/volunteers should be aware that they could be drawn into an investigation of child pornography or obscene images if they are linked to someone under investigation through a social networking site. They should inform the Headteacher/Principal/CEO immediately if they are contacted by the Police or other investigators.

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.'

If cyberbullying does take place, employees/volunteers should keep records of the abuse, text, e-mails, website or instant message and should not delete. Employees are advised to take screen shots of the messages or web page and make a note of the time, date and place of the site.

Employees/volunteers are encouraged to report any and all incidents of cyberbullying to their line manager. 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.

If the employee/volunteer becomes aware of a student being subject to cyberbullying, they should raise it with their line manager or Headteacher/Principal.

Twitter

Twitter is used as the principle means of social media to provide effective communication for students and parents/carers including information on the daily news and events in each school within Severn Academies Educational Trust.

Twitter will continue to be used to inform all stakeholder of a wide range of relevant school information such as events and trips and share links to relevant resources that may be of interest. Moreover, Twitter will be used to celebrate success and to actively promote the excellent work that takes place in all schools on a daily basis.

Twitter accounts are strictly set up with privacy settings for educational purposes is used as a **one-way channel of communication.** Followers are asked not to reply as the school will not respond. Whilst School and Trust Twitter accounts will remain 'open' to the public to encourage retweeting, monitoring of followers and their messages related to the School/Trust will take place on a regular basis. The School/Trust reserves the right to remove messages and block individuals or organisations should the need arise.

Should anyone wish to contact a school they are asked to use the normal channels of communication.

Safe and effective use of Twitter is supported through each school's Acceptable Use Policy.

Guidance:

- For students, parents/carers who do not have outside access to the Twitter social networking site, the same information will be readily available for you to collect through other means, such as from the school office, or through the school Intranet. There will be no reliance on Twitter to find out information regarding specific events and Twitter will only act as a secondary information tool.
- Images of students will be posted in accordance with the 'Permission for Photographs & Videos in School' policy. If any image is planned to be shared the students involved will all be made aware before it goes live. If consent is withdrawn, the image will be deleted and not distributed further.

Facebook

Facebook is used by our SCITT & TSA to promote their vision. This is their principle means of social media for information regarding latest events and training sessions. Facebook allows for live videos to be recorded and shared with your followers so they can see what's happening now. Also, on Facebook you can promote upcoming events by paying a small fee and by setting a maximum spend this can help save overspending in the budget.

Instagram

Instagram is used by our SCITT & TSA to promote their vision. This is another one of their means of social media for information regarding latest events and training sessions. Instagram allows for live videos to be recorded and shared with your followers so they can see what's happening now. Pictures can be posted for a short time of 24 hours and are then saved to the archive section which is only visible to the account holder.
If you have any doubts about any of the aforementioned, you should seek advice from your Headteacher/Principal/CEO.

Photograph and Video Consent Form (template)

Photographs, videos and other ‘media’ is used for the purpose of promoting the Trust and all schools within the Trust, and to publicly showcase the successes and achievements of students. This includes a wide range of promotional publications including newsletters, advertising, School/Trust websites, displays, promotional videos, digital signage and information screens, newspaper articles and social media.

In keeping with General Data Protection Regulations (GDPR) 2018 we would like your consent to take photos and/or videos for use in promoting the School/Trust and to celebrate student successes and achievements. The name and age/year group of your child will be used where appropriate and relevant, including newsletters and newspaper articles.

Please choose and tick one of the choices below and return to the School Office by [INSERT DATE]

If you prefer not to give consent to some or all uses, we will ensure your requirements are met.

I consent	I do not consent	to allowing the use of photographs/videos of my child in and around school in places that might be seen by visitors
I consent	I do not consent	to allowing the use of photographs/videos of my child in wider marketing materials including School/Trust newsletters, promotional videos, prospectuses and publicity materials
I consent	I do not consent	to allowing the use of photographs/videos of my child on the School/Trust website and social media sites

Please note, if you change your mind at any time and wish to withdraw consent, you can let us know by informing the school office on [PHONE NUMBER] or e-mail [E-MAIL ADDRESS].

Why are we asking for your consent again?
You may be aware that new data protection regulations came into effect from 25 May 2018, the General Data Protection Regulations (GDPR). To ensure we are meeting the new requirements, we need to refresh your consent to take and use photos/videos of your child. We really value using images of students to be able to showcase what students do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Student’s name: ____

Year/Form Group/Class: ______________________________________

Name of Parent/Carer: _______________________________________

Signed (Parent/Carer): _______________________________________

Date: ____