SEVERN ACADEMIES
Educational Trust

Electronic Communication Policy

May 2023

Contents: **Page No.**

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Education Act 2002
- General Data Protection Regulations (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Child Protection and Safeguarding Policy
- Critical Incident Policy
- Code of Conduct Policy
- Acceptable Use Agreement

2. 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.

3. 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
- TikTok
- Snapchat

- LinkedIn
- Mailing lists

4. 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 the Directors and Members of 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.
- You must not post images or information about anyone who has not given permission. If you are unsure, don't post.

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'

- Staff representing the Trust or Trust school online, eg through blogging or their social media accounts, will express neutral opinions and will not disclose any confidential information regarding the Trust/Trust school, or any information that may affect its reputability.
- Will not use Trust/Trust school-owned mobile devices to access personal social networking sites.
- Do not make comments about the Trust or any school, or claim to represent the views of the Trust or each school on personal social media.
- 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 Trust schools may consider to be in conflict with their values and principles.
- Will not communicate with students or parents over personal social networking sites.
- Never make a 'friend' (or equivalent) of current students or parents 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.
- Staff will not post or upload any images and videos of students, staff or parents on any Trust/Trust school website or social media without consent from the individual(s) as set out in the Trust Photography and Video Policy.
- 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.
- 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.

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 and 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.
- Staff will ensure they apply the necessary privacy settings to any social networking sites and their accounts are 'locked' down so they are private or unlisted.
- 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. Use of personal phones should be avoided. Should the need arise for telephone calls to be made from a personal phone (landline or mobile phone) the telephone number the call is being made from should be withheld 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 platforms such as 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 publicly 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.

Facebook

Facebook is being developed in our schools as the principle means of social media to provide effective communication for pupils and parents/carers and other stakeholders including information on the daily news and events in each school within our Trust and most importantly to celebrate success and achievement and the excellent work that takes place in all schools on a daily basis and promote their vision and values.

Facebook is deemed the most effective means of reaching out into our communities to boost the profiles and reputations of our schools and of the Trust, SCITT and TSA. Schools are also encouraged to use Messenger alongside Facebook in order to reach contributors privately as and when required.

Each school is to have/has a trained 'digital champion'. This is a paid responsibility to ensure Facebook and other forms of social media are used and monitored regularly, responsibly and effectively.

Questions posted by contributors should be answered and positive comments appreciated. Negative comments should also be addressed; depending on the nature of the comment this may be addressed through Messenger or by a request to call the school.

The School/Trust reserves the right to remove any insulting, racist, homophobic or other seriously derogatory comments and to block individuals or organisations from Facebook or any other social media sites should the need arise.

The reporting of absenteeism is not allowed through Facebook or any other social media. Neither are any safeguarding issues to be reported/discussed through social media.

Facebook allows for live videos to be recorded and shared with followers so they can see what's happening now and we are encouraging our schools to post more videos as they receive the greatest amount of engagement.

Also, on Facebook we are encouraging schools to promote upcoming events using 'boost' to target particular groups within the community. There is a small fee that can be set to a maximum spend.

The Trust and our schools are encouraged to use Facebook for recruitment, reaching a targeted audience for far less cost than traditional forms of advertising.

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

Instagram
The use of Instagram is also being developed across our schools to promote their vision, celebrate successes/achievements, the excellent work that goes on in schools and to disseminate information It is also used by our SCITT & TSA to promote their vision, latest events and training sessions. Instagram allows for live videos to be recorded and shared with 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.

Twitter
Twitter accounts are strictly set up with privacy settings for educational purposes is used as a **one-way channel of communication.** 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. Should anyone wish to contact a school they are asked to use the normal channels of communication.

LinkedIn
The use of LinkedIn is being developed by the Trust/Trust schools to assist with recruiting the best staff……..

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

Guidance:
- For students, parents/carers who do not have outside access to Facebook, Instagram or Twitter, the same information will be readily available for them to collect through other means, such as from the school office, or through the school Intranet. There will be no reliance on social media to find out information regarding specific events and social media 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 you have any doubts about any of the aforementioned, you should seek advice from your Headteacher/Principal/CEO.

5. Access to inappropriate content

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 content regarding 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.

6. 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.

7. Effective e-mail communication

E-mails are the principle means of written communication between staff in all schools and between schools in the Trust. Therefore, it is increasingly important that e-mails are used timely and appropriately to ensure effective work practices are in place and to enhance staff well-being. This includes considering appropriate content and tone, the timing of sent e-mails and the management of the volume of e-mails received.

Before using e-mail:

- Consider whether it is the most appropriate or timely method of communication for the situation. In some circumstances other communication forms, such as a phone call or short meeting, may be better and should be considered in the first instance.

Your decision on whether or not to use e-mail should be based on factors such as the subject matter, availability of recipient and speed of response required.

- In essence, please do not expect recipients to read and/or respond outside of normal working hours. A consideration might be to draft an e-mail in readiness to send during normal working hours.

Addressing messages:

- Only send messages to staff who actually need to know the information contained.
- Only include recipients in the "To" field who are expected to act or take decisions based on the message content.
- Include recipients in the "CC" field for information only and consider carefully whether these recipients really need to know.
- Use the "reply all" function with care. It is unlikely that everyone included in the original message will need to know your reply – avoid information overload.

Content and tone:

- You should use neutral, professional language and tone - assume that anything you write will be published.
- Avoid ill-advised comments on individuals, the trust, or other schools/organisations and ensure that you differentiate between fact and opinion
- Avoid angry e-mails – monitor the tone of the message and consider a delay, followed by a re-read before finally sending. Take care to ensure that the message is inoffensive and cannot be construed as harassment, discriminatory, abusive or offensive.

Structure and grammar:

- You should take the same care over structure, spelling, grammar and punctuation when writing an e-mail message as you would with a letter or memo. Professionalism extends to all forms of communication. In particular, you should: Use plain English as far as possible and avoid abbreviations; use paragraphs to structure information; position important information at the beginning of the message; re-read to check spelling and grammar before sending (the spelling and grammar checking function can help with this but is not a substitute for proof reading).

The use of attachments:

- The use of attachments to circulate information internally presents problems through the resulting proliferation of duplicate information in mail folders across the organisation (which must then be managed) and the increased use of server space.

Managing your Inbox:

- Many staff who receive large volumes of e-mail may find managing their mailbox a difficult and onerous task, however there are steps that can be taken to alleviate this. There is no "right" way to organise a mailbox and you must follow a method that works best for you. Allocating a fixed period of time in your schedule to read through and sort messages is an approach to help you manage your messages; this could be a small amount of time at the end of each day or a short period once a week.

Out of office:

- Appropriate arrangements for dealing with your e-mail when you are out of the office for an extended period are essential to enable the effective conduct of our business

and to ensure that we meet our legal obligations. As a matter of good practice, you should always set an out of office message indicating when you will return and providing an alternative point of contact.

Sensitive subject matter:

- Managers should avoid unnecessary use of sensitive subject matter including e-mail for discussion of employee performance issues. This limits the risks of messages being mis-sent and the creation of unnecessary records which are disclosable under information access legislation. Such matters may be more appropriately dealt with through face to face discussion, with records of meetings created as necessary and in accordance with the relevant procedure.