Social Media Policy

Document provenance

This policy was approved by as follows –	
Approver: Executive Leadership Team (ELT)	Date of Approval: June 2020
ELT Owner: Chief Operating Officer	Date of Review: June 2022
Unless there are legislative or regulatory changes in the interim, this policy will be reviewed every two years. Should no substantive changes be required at that point, the policy will move to the next review cycle.	

This policy should be read as new.

The **purpose of this policy** is to set out obligations on the part of E-ACT staff regarding the acceptable use of Social Media. It also includes guidance about steps the Trust may take to ensure compliance with this policy.

Related policies and guidance:

- Data Protection Policy[1]
- Information Security Policy[2]
- Online Safety Policy[3]
- Social Media Guide (Insight)[4]

[1] https://insight.e-act.org.uk/policies/data-protection-policy-staff
[2] https://insight.e-act.org.uk/policies/information-security-policy
[3] https://insight.e-act.org.uk/policies/online-safety-policy
[4] https://insight.e-act.org.uk/system/files/Social%20media%20guidelines_0.pdf

Social Media Policy

1. Introduction and Purpose

1.1. Policy Statement

1.1.1. Social media gives the Trust the ability to easily promote great news and to grow our networks, and the Trust encourages responsible of social media.

1.1.2. Whilst recognising its benefits, this policy sets out the principles that all staff are expected to follow when using social media, both on behalf of the Trust and when using personal accounts.

1.1.3. Please note that this policy does not form part of any employee's contract of employment and it may be amended at any time.

1.1.4. In addition to this policy, please see the Trust's social media guidelines for advice on how to get the best from an E-ACT Trust-affiliated social media account. These guidelines are available on our staff intranet site - Insight. The guidelines cover such topics as how to plan social media activity, growing followers and when to post for maximum impact.

1.1.5. However, the Trust is aware, that the use of social media can pose risks to our ability to safeguard young people. Its misuse can also impact on our legal obligations and our ability to protect confidential information.

1.2. The purpose of this Policy

1.2.1. Through this policy, we aim to promote innovation through the use of social media within a framework of good practice that is set by the Trust.

1.2.2. We aim to:

- Safeguard and protect pupils;
- Ensure that the reputation of the Trust is protected.;
- Ensure that all E-ACT employees are operating within the Trust's social media framework.

2. Scope

2.1. Who is covered by this policy?

2.1.1. This policy covers all E-ACT employees working at all levels and grades.

2.1.2. It also applies to E-ACT Ambassadors, consultants, contractors, casual and agency staff, and volunteers, collectively referred to as 'staff' in this policy.

2.1.3. Third parties who have access to our communication systems and equipment are also required to comply with this policy.

2.2. **Scope of the Policy**

2.2.1. This policy deals with the use of all forms of social media and all other internet posting sites.

2.2.2. It applies to the use of social media for both business and personal purposes during working hours or otherwise. The policy applies regardless of whether social media is accessed using our E-ACT IT facilities and equipment, or equipment belonging to members of staff.

2.2.3. The impact and social media platforms on the internet are fast paced and change rapidly, so the policy does not attempt to cover all circumstances. Staff must apply common sense and professional judgement when faced by situations not covered by this document. However, staff are required to seek advice if they are unsure of how to use a particular aspect of social media or have concerns and need additional guidance. Please contact the Director of Communications, Humayon Pramanik (Humayon.Pramanik@E-ACT.org.uk) with any questions.

3. Legislation and Regulation

3.1. Anything shared through social media is subject to copyright, data protection and freedom of information legislation.

3.2. Where a person can be identified from a photograph or a video, then that piece of media contains their personal data. Its use is therefore covered by Data Protection Legislation.

3.3. **Compliance with related policies and agreements**

3.3.1. Social media should never be used in a way that breaches any of the other E-ACT policies. Employees are prohibited from using social media to:

- Breach our IT Acceptable Use Policy;
- Breach any obligations they may have relating to confidentiality;
- Breach our disciplinary rules;
- Harass or bully other staff or pupils in any way or breach our Code of Conduct Policy and our Behaviour, Anti Bullying and Exclusions Policy;
- Unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policies;
- Breach our Data Protection Policy
- Breach our Information and Records Retention Policy;
- Breach any other laws or ethical standards.

3.3.2. Employees who breach any of the above policies may be subject to disciplinary action up to and including termination of employment.

4. Policy Statement

4.1. **Breach of this policy**

4.1.1. Any misuse of social media should be reported to the Headteacher (academy staff), Regional Operations Director (regional staff), and the Director of

Communications (national staff). Questions regarding the content or application of this policy should be directed to staff in these roles.

4.1.2. Any member of staff suspected of committing a breach of this policy will be required to cooperate with an investigation. This may involve handing over relevant passwords and login details.

4.1.3. Staff may be required to remove posts which are deemed to constitute a breach of this policy

4.1.4. Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

4.2. **Business use of social media**

4.2.1. If as part of your role at E-ACT your duties require you to communicate on behalf of the Trust in a social media environment, you must first seek approval from your line manager who may require you to undergo training before you do so.

4.2.2. It may be that you maintain your academy's Facebook page with updates for parents or you are asked to run the academy's Twitter account. Please note that your line manager can impose certain requirements and restrictions with regard your activities.

4.2.3. You must only use Trust owned equipment to post to on an E-ACT social media account.

4.2.4. Please also refer to our IT Acceptable Use Policy for further information.

4.3. **Monitoring**

4.3.1. The contents of our IT resources and communications systems are the property of the Trust. This means that:

- We reserve the right to monitor, intercept and review, without further notice, all staff activities using our IT resources and communications systems.
- Any message, file, data, document, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems can be monitored by the Trust.
- This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

4.3.2. You consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. For further information please refer to our IT Acceptable Use Policy.

4.4. **Requirements for setting up a trust-affiliated account**

4.4.1. If you would like to set up a social media account that is in anyway affiliated to the Trust or one of its academies or if you have already set up such an account, you must contact the Director of Communications using the email address - Humayon.Pramanik@E-ACT.org.uk.

4.4.2. In your email to the Director of Communications, provide the following detail:

- The name of the social media platform
- Username and password
- The details of two account holders (every account must have two administrative contacts). You must not use your personal e-mail address for professional social media activities.

4.4.3. The Director of Communications will provide a short induction to best practice in using social media fur all matters relating to your professional role as an E-ACT member of staff.

4.5. **Request for comment through social media**

4.5.1. If you are contacted for comment about the Trust for publication anywhere including in any social media or news outlet, direct the enquiry to the Director of Communications (Humayon.Pramanik@E-ACT.org.uk) and do not respond without written approval.

4.6. **Putting activity on hold**

4.7. If it is deemed necessary, for example if one of our academies is experiencing a crisis event, the Trust may request that no further social media posts are made for a period of time.

4.8. **Recruitment and social media**

4.8.1. The Trust will not, either themselves or through a third party, conduct searches on applicants on social media.

4.8.2. Conducting such searches during a recruitment and selection process may lead to a presumption that an applicant's protected characteristics played a part in a recruitment decision. This is in line with the Trust's Equal Opportunities Policy.

4.8.3. Exceptions to this rule apply only if an individual has put their details on a social media website for the purpose of attracting prospective employers.

4.8.4. Furthermore, staff should never provide references on or through use of social media sites. Such references can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

5. Responsible use of social media

5.1. The following section of this policy provides staff with common sense guidelines and recommendations for using social media responsibly and safely. They apply to both personal and trust-affiliated accounts.

5.2. **Safeguarding children and young people:**

- You must not communicate with pupils over social media sites.
- You must never send a direct message to a pupil through a social media account.
- Staff must not respond to any direct communication from a pupil.
- Pupils' personal accounts should never be tagged in a social media post.
- Staff must not accept any current pupil of any age as a follower on a personal account.
- Any communication received on a personal account from a pupil must be reported to the Designated Safeguarding Leader in an academy or in the regional team.
- If a social media platform is being used as a way for pupils to collaborate with a member of staff as part of an academy project or specific subject, that account must me made private.
- You must block unwanted communications from pupils.
- You should not interact with any ex-pupil of the Trust who is under 18.
- Privacy settings should be set so that age restrictions are set at 13+. Children under 13 are not legally allowed to create social media accounts.
- You should enable a profanity filter.
- Any sharing of links to external sites must be appropriate.
- Abusive or threatening posts should be reported to your manager and the Director of Communications (Humayon.Pramanik@E-ACT.org.uk)
- Avoid posting anything on a personal account that you do not want your pupils to see and consider stricter privacy settings.
- only trust owned equipment to post to an E-ACT social media account.

5.3. **Protecting our reputation:**

- Staff must not post disparaging or defamatory statements about the trust, pupils, parents or carers, trustees, staff, suppliers or any other Trust Stakeholders.
- Staff should avoid posting messages that might be misconstrued in a way that could damage our reputation.
- If you disclose your affiliation as an employee of our Trust on a personal account, you must also state that your views do not represent those of your employer.
- You should ensure that your profile and any content you post are consistent with the professional image you wish to present to pupils and colleagues.
- Avoid posting comments about sensitive trust-related topics.
- If you are contacted for comment about the Trust by the press or some other external agency, staff must direct the enquiry to the Director of Communications and do not respond without approval.
- Deal with any complaints by offering dialogue through a more appropriate channel. Direct message the complainant with alternative contact details to avoid any awkward public conversations.

5.4. **Respecting intellectual property and confidential information**:

- Remember that anything shared through social media is subject to copyright, data protection and freedom of information legislation.
- Staff must not post anything that could jeopardise our confidential information and intellectual property.
- Staff should avoid misappropriating or infringing the intellectual property of other companies and individuals.
- Do not use our logos, brand names, slogans or other trademarks or post any of our confidential or proprietary information without prior written permission.
- Respecting colleagues, pupils, parents and carers, trustees and other stakeholders:
- Do not post anything that your colleagues or our pupils, parents and carers, trustees and other stakeholders would find offensive including discriminatory comments, insults, threats or obscenity.
- Do not post anything related to your colleagues, our pupils, parents and carers, trustees, and other stakeholders without their written permission.
- Circulating chain letters or other spam is never permitted.
- Circulating or posting commercial, personal, religious or political solicitations or promotion of outside organisations unrelated to the trust's business are prohibited.

5.5. If you are uncertain or concerned about the appropriateness of any posting refrain from making the communication until you discuss it with the Headteacher, Regional Operations Director or the Director of Communications.

6. Data Protection

6.1. Where a person can be identified from a photograph or a video, that piece of media contains their personal data. Its use is therefore covered by data protection legislation.

6.2. If posting to a trust-affiliated account (an academy Facebook page or a regional Twitter account for example) **consent must therefore be sought** using the trust's consent form before any pupil can be photographed and featured in a social media posting:

- For pupils in Year 6 and below, consent should be sought from parents.
- For pupils in Years 7 to 11, consent should be sought from both pupils and parents.
- For pupils in the sixth form, consent need only be obtained from the pupil unless you consider there is a particular reason to also speak to parents.

6.3. Photography consent forms are available on Insight Intranet.

6.4. Note that only Trust owned equipment may be used to capture photography, video or any other media when posting in a professional capacity.

6.5. Please speak to your Headteacher if you require the use of a Trust owned device.

7. Training

7.1. Business use of social media

7.1.1. If as part of your role at E-ACT your duties require you to communicate on behalf of the Trust in a social media environment, you must first seek approval from your manager who will require you to undergo training before you do so.

8. Responsibilities

8.1. Personnel responsible for implementing this policy

8.1.1. All staff have a responsibility to follow this policy and should ensure that they take the time to read and understand it.

8.1.2. The Board of Trustees has overall responsibility for ensuring that the policy is implemented effectively. They delegate this day-to-day responsibility to the:

- Headteachers at academy level
- Regional Operations Directors at regional level
- The Executive Leadership Team at national level.

9. Monitoring and Compliance

9.1. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change lies with the CEO and the Director of Communications.

9.2. The Regional Directors are also responsible for reporting at Regional Performance Boards (RPBs) on the impact of our policies and report by exception if items in this policy need reviewing earlier than planned in the policy cycle.