Raleigh EDUCATION TRUST

Human Resources Policy

Social Media Policy

CEO approval:	Sean Kelly	September 2023
LGB Cluster ratification		
Joint Negotiating Council (JNC) consultation (where applicable):		September 2023
Last reviewed on:	September 2023	
Next review due by:	September 2025	

Contents

1. Policy statement 3
2. Who is covered by the policy? 3
3. Scope and purpose of the policy 3
4. Responsibility for implementing the policy 4
5. Compliance with related policies and agreements 4
6. Personal use of social media 5
7. Monitoring and data protection 5
8. Business use of social media 6
9. Recruitment 6
10. Responsible use of social media 6
11. Review of policy 8

1. Policy statement

1.1 We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Instagram, Linkedin, Snapchat, Tik-Tok, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our ability to safeguard children and young people, protect confidential information and reputation, and can jeopardise our compliance with legal obligations. This could also be the case where social networking activities are conducted on-line outside work.

1.2 Employees using social media are also potentially at risk of others misunderstanding the intent behind online communications or blurring of professional boundaries between children and young people and their parents or carers. This policy therefore sets out the Trust's expectations regarding the use of social media.

1.3 To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, and that the use of personal devices does not have an adversary impact on our business we expect employees to adhere to this policy.

1.4 This policy does not form part of any employee's contract of employment, and it may be amended following consultation with the recognised trade unions.

2. Who is covered by the policy?

2.1 This policy covers all employees working at all levels and grades. It also applies to consultants, contractors, casual and agency staff and volunteers (collectively referred to as staff in this policy).

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

3. Scope and purpose of the policy

3.1 This policy addresses the use of all forms of social media, including Facebook, Instagram, LinkedIn, Snapchat, Tik-Tok, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

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

3.3 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. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve providing relevant passwords and login details.

3.4 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

4. Responsibility for implementing the policy

4.1 The Trust Board has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the CEO. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with CEO.

4.2 All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

4.3 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Principal / CEO. Questions regarding the content or application of this policy should be directed to Principal / CEO.

5. Compliance with related policies and agreements

5.1 Social media should never be used in a way that breaches any of our other policies, including our Code of Conduct which states our expectations and responsibilities of our employees. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) breach our ICT User Policy;

b) breach our obligations with respect to the rules of relevant regulatory bodies;

c) breach any obligations they may have related to confidentiality;

d) breach our Disciplinary Rules;

e) defame or disparage the Academy / Trust or its affiliates, trustees, members, students, parents and carers, staff, business partners, suppliers, vendors or other stakeholders;

f) harass or bully other staff in any way;

g) unlawfully discriminate against other staff or third parties or breach our Equality and Diversity Policy;

h) breach our Data Protection Policy (for example, never disclose personal information about a colleague or pupil online);

i) breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

5.2 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Academy / Trust and create legal liability for both the author of the reference and the Academy / Trust. Further guidance regarding the provision of references is included in the Trust's Reference Policy.

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

6. Personal use of social media

6.1 Blogging and accessing social networking sites at work or at home using Trust equipment is not permitted, unless for professional purposes and has been authorised by an appropriate individual.

6.2 While using social media at work, 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 Academy / Trust's business are also prohibited.

6.3 It is not acceptable to communicate on social media about the Academy / Trust or any member of the Trust's community in or out of work on personally owned equipment.

6.4 To ensure the safety and welfare of pupils in our care, personal mobile phones, cameras and video recorders must not be used when children are present. Mobile phones must be kept in a secure place, switched off and not be accessed during contact time with pupils. There may be exceptions which have been discussed and agreed with your line manager / Principal, however, their use must be out of the view of pupils.

7. Monitoring and data protection

7.1 The contents of our IT resources and communications systems, held in whatever media, including information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones, relating both to the Employer's own education provision or any pupils, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, 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.

7.2 Providing there is sufficient reason and foundation, we may monitor intercept and review, without further notice, employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and are for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies. Line managers should liaise with Colwyn Technologies to agree monitoring processes and duration to be undertaken and how information will be presented by IT.

7.3 We will comply with the requirements of Data Protection Legislation (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998) in the monitoring of our IT resources and communication systems Monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.

7.4 In line with the requirements of Data Protection Legislation, we may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice. Records will be kept in accordance with our Workforce Privacy Notice, our Retention and Destruction Policy.

7.5 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Academy / Trust.

7.6 For further information, please refer to our ICT User Policy and Data Protection Policy.

8. Business use of social media

8.1 If your duties require you to speak on behalf of the Academy / Trust in a social media environment, you must still seek approval for such communication from the Principal or the CEO who may impose certain requirements and restrictions with regard to your activities.

8.2 Likewise, if you are contacted for comments about the Academy / Trust for publication anywhere, including in any social media outlet, direct the enquiry to the Principal or CEO and do not respond without written approval.

8.3 The use of social media for business purposes is subject to the remainder of this policy.

9. Recruitment

9.1 Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), the Academy / Trust will not, either themselves or through a third party, conduct searches on applicants on social media. This is because conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the Trust's Equality and Diversity Policy.

10. Responsible use of social media

10.1 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely and in order to protect staff and the Academy / Trust.

10.2 Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case where social networking activities are conducted on-line outside work.

10.3 Safeguarding children and young people:

a) You should not communicate with pupils over social network sites. You must block unwanted communications from pupils. Incidents should be reported through CPOMS.

b) You should never knowingly communicate with pupils in these forums or via personal email account or using your school e-mail account where the communication is non-school related.

c) You should not interact with any ex-pupil of the Academy / Trust who is under 18 on such sites.

d) Communication with pupils should only be conducted through our usual channels. This communication should only ever be related to our business.

e) Anyone whose practice deviates from our commitment to safeguarding children and young people 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.

10.4 Protecting our business reputation:

a) Staff must not post obscene, indecent, racist or offensive remarks or comments on social media nor should you entice others to do so. Staff must not make disparaging or defamatory statements about:

i. our Academy / Trust;

ii. our students or their parents or carers;

iii. our trustees / members or staff;

iv. suppliers and vendors; and

v. other affiliates and stakeholders,

b) Staff should also avoid social media communications that might be misconstrued in a way that could damage our Academy / Trust's reputation, even indirectly. Staff must not make social media posts that are defamatory or which are intended to offend, annoy, harass, bully or intimidate another person or persons.

c) Staff should make it clear in social media postings that they are speaking on their own behalf and not as a representative of the Trust. Write in the first person and use a personal e-mail address when communicating via social media.

d) Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including the Academy / Trust itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

e) If you disclose your affiliation as an employee of our Academy / Trust, you must also state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer". You should also ensure that your profile and any content you post are consistent with the professional image you present to pupils and colleagues.

f) Avoid posting comments about confidential or business-sensitive Academy / Trust-related information, topics or images, such as our performance. Even if you make it clear that your views on such topics do not represent those of the Academy / Trust, your comments could still damage our reputation and compromise the security of the Trust.

g) You should be aware of on-line identity fraud and be cautious when providing personal information about yourself which may compromise your personal safety and security.

h) You should ensure that high levels of privacy are set if you choose to use social media.

i) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your line manager / Principal.

j) If you see content in social media that disparages or reflects poorly on our Academy / Trust or our stakeholders, you should print out the content and contact the Principal / CEO. All staff are responsible for protecting our Academy / Trust's reputation.

10.5 Respecting intellectual property and confidential information:

a) Staff should not do anything to jeopardise our confidential information and intellectual property through the use of social media.

b) In addition, staff should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the Academy / Trust, as well as the individual author.

c) Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

10.6 Respecting colleagues, students, parents and carers, trustees / members and other stakeholders:

a) Do not post anything that your colleagues or our pupils, parents and carers, Trustees / Members and other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

b) You must not post images of staff, pupils or anyone directly connected with the Academy / Trust whilst engaged in Academy / Trust activities.

c) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

11. Review of policy

11.1 This policy is reviewed every 2 years by the Trust in consultation with the recognised trade unions. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Appendix A – Guidance – Using Social Media

1. Keeping safe on-line

1.1 Some social media sites and other web-based sites have fields in the user profile for job title, etc. If you are an employee of the Trust, you should not put any information onto the site that could identify either your profession, the Academy / Trust where you work. In some circumstances, this could damage the reputation of the Academy / Trust and your profession.

1.2 Staff need to be aware of including 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 the work environment. It also reduces the potential for identity theft by third parties.

1.3 All staff, particularly new staff, should review their social networking sites when they join the Trust to ensure that information available about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves or the Trust if they are published outside the site. Privacy settings should then be set at the highest level.

2. Protection of personal information

2.1 Staff should not give their personal e-mail address to pupils or parents. Where there is a need for communication to be sent electronically, the Trust e-mail address should be used. Equally, staff should keep their personal phone numbers private and not use their own mobile phone to contact pupils or parents in a professional capacity.

3. Cyber-bullying

3.1 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". All staff 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.

3.2 If cyber-bullying does take place, staff should keep records of the abuse and should not delete it but take screen prints including the time, date and place of the site. Staff are encouraged to report all incidents of cyber-bullying to their line manager / Principal. All such incidents will be taken seriously and will be addressed in consideration of the wishes of the person who has reported the matter.