KALEIDOSCOPE
Multi Academy Trust

Social Media and Networking Policy

October 2025

Based upon the North Somerset Model Policy

Approved by: **Next Review:**	Kaleidoscope Trust Board October 2026	**Date:** October 2025

CONTENTS

Overview and Introduction	3
Scope and General Principles	3
Responsibilities	4
Use of Social Networking Sites	6
Use of School Sites, Pages and Spaces	8
Equal Opportunities	9
Relevant Policies / Guidance	9
Legislation	9

SOCIAL MEDIA AND NETWORKING POLICY

1 OVERVIEW AND INTRODUCTION

1.1 The purpose of this policy is to:

- Ensure the exposure to legal and governance risks of Kaleidoscope Multi-Academy Trust schools (henceforth known as 'the school') is minimised;
- Enable colleagues at the school to use social networking sites safely and securely;
- Ensure that colleagues are aware of their responsibilities in connection with the use of social networking sites and of the risks associated with the inappropriate use of social networking sites and any impacts in relation to their employment;
- Safeguard colleagues at the school in connection with the use of social networking sites and minimise the risk that they make themselves vulnerable to allegations
- Ensure the Trust Board and Local Governing Body maintains its duty to safeguard children, the reputation of the school and those who work for it, the wider community and the Local Authority.

2 SCOPE AND GENERAL PRINCIPLES

2.1 In this Policy colleague' means all individuals engaged by the school in a paid or voluntary capacity including parent helpers and governors, those on work experience placements and agency colleagues. Third parties acting on behalf or in partnership with the school are also expected to adhere to this guidance.

2.2 This Policy applies to social networking sites, personal web pages, personal space provided by internet providers and internet presences which make available personal information (including images) and opinions to the general public *including* but not limited to Facebook, Pinterest, Snapchat, WhatsApp, Instagram, MSN, Twitter/X, YouTube, blogs, wikis, forums, bulletin boards, chatrooms, multiplayer on-line gaming, virtual worlds and instant messenger.

2.3 In this Policy 'pupil' should, where relevant, be taken to include any child/young person attending the school. If a colleague has a difficulty complying with this Policy (for example if they are related to a pupil attending the school) they should declare this relationship to the Headteacher. This policy does not cover relationships which are not facilitated directly or indirectly by the school.

2.4 This Policy will be part of the Induction programme for all new colleagues at the school and on its introduction, will be shared with all existing colleagues.

2.5 The Trustees and Local Governing Bodies do not discourage colleagues at the school from using social networking sites. However, all colleagues at the school should be aware that the Local Governing Body will take seriously

any occasions where the services are used inappropriately. They will report these concerns to the Trust Board.

2.6 Instances of on-line bullying and harassment will be regarded as a serious matter and will be dealt with under the school's Disciplinary Policy. Any school colleague who is being bullied or harassed on-line or is the subject of inappropriate messages or false allegations should report this to the Headteacher / their Line Manager. Please also see the School's ICT Policy for expectations around the level of use of Social Networking sites.

2.7 In the event that this Policy is not followed or any instances of the inappropriate use of social networking sites are brought to the attention of the School, these may be investigated under the School's Disciplinary Policy and depending on the seriousness of the matter disciplinary action may be taken which may result in dismissal. A serious breach of the Policy may be regarded as gross misconduct, leading to summary dismissal.

2.8 Where any allegations have a children's safeguarding dimension (that is, where an individual has:

- behaved in a way that has harmed a child, or may have harmed a child;
- possibly committed a criminal offence against or related to a child or
- behaved towards a child or children in a way that indicates he or she would pose a risk of harm to children)

the Designated Officer for Allegations (DOFA) (formerly LADO) must be contacted via the Social Care's Single Point of Access on 01275 888808 at the earliest opportunity and the Allegations of Abuse procedure outlined within the DfE's *Keeping Children Safe in Education* guidance must be followed (this is available on the NSESP website or on the DfE website at: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

2.9 Where there are concerns as to the legality of any activity or behaviour the School or Local Authority will be obliged to inform the police.

3.0 RESPONSIBILITIES

3.1 **The Trust Board shall:**

- Ensure that the MAT has up to date policies and procedures and agrees these.
- Ensures that all policies and procedures are agreed by Local Governing Bodies.
- Monitor and audit any breaches of policies or concerns. Trustees will ensure actions follow those outlined in this and other safeguarding policies.

3.2 **The CEO shall:**

- Ensure policies are up to date and presented to the Trust Board.
- Support schools where needed.
- Act if there are breaches of policy.
- Update the Trust Board on safeguarding issues.

3.3 **The Local Governing Body shall:**

- Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites;
- Ensure that all colleagues at the school have access to this policy and that colleagues including new colleagues are made aware of it.

3.4 **Headteachers/Line Managers shall:**

- Be familiar with this policy and guidelines and ensure that colleagues understand the policy and their own responsibilities;
- Ensure that colleagues at the school are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them;
- *Make partners and any other third parties aware of this guidance where relevant.*
- Instigate disciplinary procedures where appropriate to do so;
- Seek advice where necessary from Human Resources and / or Social Care's Single Point of Access on the approach to be adopted if they are made aware of any potential issue.

3.5 **Colleagues at the school shall:**

- Comply with all the school's relevant policies, guidance and codes of practice and relevant national guidance.
- Behave safely, responsibly and professionally at all times on-line and in connection with the use of social networking sites.
- Ensure that all communication with pupils (including on-line communication) takes place within clear and explicit professional boundaries as set out in the Safer Recruitment Consortium's *Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings* using school-based systems.
- Report any concerns that any colleague(s) is/are not acting in accordance with this Policy to their line manager/the Headteacher/the school's designated safeguarding lead.
- Act in accordance with the school's Whistleblowing Policy
- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with their manager or the Headteacher if they are unsure.
- Co-operate with management in ensuring the implementation of this policy.
- Respect the privacy and feelings of others.
- Keep a professional distance from pupils and ex-pupils of school age and ensure a clear separation of the private social lives of colleagues at the school and those of pupils and ex-pupils of school age.
- Report to their Headteacher, school designated safeguarding lead or line manager any occasions when a pupil attempts to involve them in on-line or social networking activity.
- Promote the safe and responsible use of the internet / social networking sites by colleagues and pupils wherever appropriate.

3.6 **Parents and third parties are encouraged to:**

- Raise any concerns that any colleague(s) at the school is/are not acting in accordance with this Policy with the Headteacher.

4.0 USE OF SOCIAL NETWORKING SITES

4.1 All colleagues at the school should follow the following guidance / procedures: *Please note: if a colleague at the school believes they will have any difficulty complying with any of the requirements below for whatever reason (for example, where they are related to a pupil), they must discuss the matter with the Headteacher / the school designated safeguarding lead. Failure to do so will be regarded as a serious matter.*

1. Colleagues at the school must not access social networking sites for personal use via school information systems or using school equipment;
2. Colleagues at the school must not accept pupils as friends or use internet or web-based communication channels to send any personal messages to pupils directly or indirectly (for example via the parents of pupils) – personal communication could be considered inappropriate and unprofessional and makes colleagues at the school vulnerable to allegations;
3. Colleagues at the school are strongly advised not to be friends (on or off line) with recent pupils (the potential for colleagues at the school to be compromised in terms of content and open to accusations makes the risk not worth taking) and colleagues at the school are also strongly advised not to be friends with pupils at other schools (on or off line) as this is likely to make them vulnerable to allegations and may be open to investigation by the Local Authority or police. Where a colleague is considering not following this advice, they are required to discuss the matter, and the implications with the Headteacher or designated safeguarding lead.
4. Any pupil-initiated communication, on-line friendships/friend requests must be declined and reported to the Headteacher or designated safeguarding lead (If a colleague receives messages on his/her social networking profile that they think could be from a pupil they must report it to their line manager/Headteacher and discuss whether it is appropriate for the colleague to contact the internet service or social networking provider so that the provider can investigate and take the appropriate action);
5. Colleagues at the school must not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details);
6. Colleagues at the school must not place/post any material (or links to any material) of a compromising nature (that is, any material a reasonable person might find obscene or offensive (such as sexually explicit or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space;
7. Colleagues at the school are advised not to write about their work but where a colleague at the school chooses to do so:
    - he/she must make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority (and all

other guidelines in this policy must still be adhered to when making any reference to the workplace)
- he/she must not discuss pupils, colleagues, parents or carers and
- he/she must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the General Data Protection Regulation (GDPR) or the Data Protection Act 2018 or disclose any information about the school/Local Authority that is not yet in the public arena;

8. Colleagues at the school must not post or share photographs of pupils under any circumstances and must not post or share photographs of colleagues or parents without their express permission;
9. Colleagues at the school must not make what could reasonably be perceived as abusive/defamatory/undermining/derogatory/critical remarks about the school/colleagues/pupils/parents/governors or the Local Authority or post anything that misrepresents or could potentially bring the school/Local Authority into disrepute;
10. Colleagues at the school must not disclose confidential information relating to their employment at the school;
11. Colleagues at the school must not link their own sites to the school website or use the school's or the Local Authority's logo or any other identifiers on their personal web pages;
12. If any colleague at the school receives media contact regarding the content of their site or is offered payment for site content which relates to the school they must consult their Headteacher/line manager;
13. Colleagues at the school must not use any internet/on-line resources to seek information on any pupil, parent or other colleague at the school other than for the purposes of legitimate monitoring of the usage of Social Networking sites by designated managers / officers.
14. Colleagues at the school must not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this
15. All colleagues must make themselves aware of and act in accordance with their duties under the DfE statutory guidance *Keeping Children Safe* as these relate to:
    - their own on-line activity
    - the on-line activity of pupils and other colleagues and
    - information of which they become aware on-line

    including their duties relating to online safety, children missing from education, child sexual exploitation, child criminal exploitation, domestic abuse, homelessness, 'honour based' violence (including FGM and forced marriage), preventing radicalisation (Prevent and Channel), peer on peer abuse and sexual violence and sexual harassment between children in school.

4.2 Keeping Children Safe in Education states: 'as part of the shortlisting process schools and colleges should consider carrying out an online search as part of their due diligence on the shortlisted candidates. This may help identify any incidents or issues that have happened, and are publicly available online,

which the school or college might want to explore with the applicant at interview. Schools and colleges should inform shortlisted candidates that on-line searches may be done as part of due diligence checks'. Such on-line searches are not compulsory. KCSIE does not refer to social media searches, only online searches. Only a general search engine (e.g. Google) search should be undertaken. Please see the Disclosure Policy for guidance relating to conducting online searches on shortlisted candidates.

4.3 The School reserves the right to take action to obtain the removal of any content posted by colleagues at the school which may adversely affect the reputation of the school (or any colleague, governor, pupil or parent at the school) or put it at risk of legal action. Should the school decide to pursue this course of action, the advice of the Local Authority's Marketing and Communications Team may be sought.

4.4 We would expect all former colleagues at the school to continue to be mindful of good children's safeguarding practice and of the school's reputation in using social networking sites.

4.5 For further information about the safe, secure and proper use of social media and networking sites, please see http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals

5.0 USE OF SCHOOL SITES, PAGES AND SPACES

5.1 All colleagues at the school should follow the following guidance / procedures:

1. The School ICT Policy / E-Safety Policy must be adhered to at all times when content is posted on the school sponsored sites/pages/spaces or on-line school communication systems/networks are used. Usage will be monitored under the ICT Policy / E-Safety Policy and any breach in this regard will result in the offending content being removed and may result in disciplinary action and any 'publishing' rights of the relevant colleague being suspended in accordance with the School's ICT Policy.
2. Content must be appropriate for use with the relevant pupils.
3. Communications or pages undertaken/run on behalf of the school must be password protected and run from the school website.
4. Colleagues at the school must not run social network spaces for pupil use on a personal basis. If a network is to be used to support pupils with coursework and as part of the educational process, professional spaces must be created by colleagues and pupils using a restricted, school-endorsed networking platform in line with school ICT and governance policies. (Specific sites can be negotiated via a license process for relevant colleagues, with specific guidelines on use and consequences for breaches of the guidelines being set out and backed by a signed undertaking from the relevant colleagues to use the sites in accordance with the guidelines.)

5. Any inappropriate behaviour by pupils on-line must be reported to the Headteacher or member of the senior leadership team and will be dealt with through the school's pupil disciplinary process.
6. Colleagues at the school must not request or respond to any personal information from any pupil unless consistent with their professional role and approved by the school.

6.0. EQUAL OPPORTUNITIES

6.1 Managers must not discriminate on the grounds of race, age, gender, disability, sexual orientation, religion or belief, gender reassignment, marriage and civil partnership, pregnancy and maternity, or other grounds and ensure that the needs of colleagues and pupils are given careful consideration when applying this Policy.

7.0. RELEVANT POLICIES / GUIDANCE

- Keeping Children Safe in Education (DfE statutory guidance)
- Guidance for Safer Working Practice (formerly DfE guidance, revised by the Safer Recruitment Consortium in 2015)
- Disciplinary Policy and Procedure
- Code of Conduct / Staff Behaviour Policy
- Safeguarding or Child Protection Policy
- Equality Scheme / Policy
- ICT Policy/Acceptable use Policy
- E-Safety Policy
- Whistleblowing Policy

8.0 LEGISLATION

8.1 The following legislation must be considered when adhering to this policy:

- Obscene Publications Act 1959
- Protection of Children Act 1988
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

Please note this list is intended to be indicative only

Date of Original: December 2012
Revisions: reference to *Keeping Children Safe* added (April 2014); reviewed and updated (January 2016); reviewed with minor updates due to issue of updated *Keeping Children Safe* guidance in para 4.1 (15) (September 2016); job title LADO updated to DOFA (November 2016); minor revisions relating to Data Protection Act being superseded by the GDPR and the Data Protection Act 2018 (Jun 2018); reviewed with minor updates due to issue of updated *Keeping Children Safe* guidance in para 4.1 (15) (September 2018)
Review Date: September 2020

All our policies and guidance can be found at www.nsesp.org Version: 7