ALDRIDGE EDUCATION

Social Media Policy

Policy Title:	Social Media Policy
Version:	June 2020
Trust Board Approval:	July 2020
Date of Next Review:	July 2021

1. Introduction and Purpose

The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to the Trust, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard, children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff employed by Aldridge Education, whether working in our schools or as part of our Central team.

The **purpose** of the policy is to:

- Encourage good practice, to protect the school/Trust and its employees, and to promote the effective use of social media as part of the school/Trust activities.
- Encourage its safe use by the Trust employees.
- Avoid personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's/Trust reputation are within the scope of this policy.
- Safeguard all children.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.
- Protect Aldridge Education from legal risks.
- Ensure that the reputation of Aldridge Education, its schools, staff, governors and trustees is protected.

While recognising the benefits of these media for new opportunities for communication, this policy set out the principles that Aldridge Education staff, visitors and contractors are expected to follow when using social media.

It is crucial that pupils, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school and Trust are safeguarded.

Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

2. Scope

This policy applies to all Trust members including, trustees, local governing bodies, all teaching and support staff, whether employed by the Trust or employed directly by the school, external contractors providing services on behalf of the school or the Trust, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the Trust/school. The policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers. These individuals are collectively referred to as 'staff members' in this policy.

This policy covers personal use of social media as well as the use of social media for official school purposes; including sites hosted and maintained on behalf of the Trust or schools within the Trust.

This policy applies to personal web space / accounts such as social networking sites (for example *Facebook*, *Myspace*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social networking sites and content sharing sites such as *flicker, Instagram* and *YouTube*. The Internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

The policy applies regardless of whether the social media is accessed using the school's IT facilities and equipment, or equipment belonging to members of staff.

3. Legal Framework

Aldridge Education is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- The Data Protection Act 2018.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- School or Trust business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Act 2013
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.
- Data Protection Act 2018

Aldridge Education could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render Aldridge Education liable to the injured party.

4. Related policies

This policy should be read in conjunction with the following school policies:

- Acceptable Use Policy
- E-safety Policy
- Safeguarding Policy
- Data Protection Policy

5. Principles – be professional, responsible and respectful

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school/Trust and your personal interests.

- You must not engage in activities involving social media which might bring Trust into disrepute.

- You must not represent your personal views on or via any school or Trust social media account unless those views are supporting and wholly in accordance with Trust or school policies and strategies.

- You must not discuss personal information about students school/Trust staff and other professionals you interact with as part of your job on social media.

- You must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, schools or the Trust.

- Aldridge Education is an apolitical organisation. You must not comment on political issues of a national or local nature, whether supporting or opposing, on a Trust or school social media account, or in such a way that a reader could believe that it the view stated was that of the school or Trust.

- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school or Trust.

6. Social Media of behalf of Aldridge Education

School and Trust social media sites should be created only for the purpose of promoting the school or Trust to its target audiences, including schools' local communities, and supporting group communications to students and parents / carers.

Social media accounts are a mass communication tool. They should not be used for one to one communication with students, and should be avoided for one to one communication with parents / carers and third party organisations. Where a parent or third party initiates a conversation via social media staff should make every effort to respond and continue communication via an appropriate one to one medium (telephone, email, letter, meeting etc).

There must be a strong pedagogical or business reason for creating official school sites to communicate with students or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputation damage.

Official school sites must be created only according to the requirements specified in **Appendix A** of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

Staff members must at all times act in the best interests of our children and young people, our schools and the Trust when creating, participating in or contributing content to social media sites.

7. Social Media for personal use

Staff members must not identify themselves as employees of school or Trust or in their personal social media accounts (except LinkedIn for work / professional related purposes. This is to prevent information on these sites from being linked to the school or Trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive front-line services.

To use social media for work purposes staff should create a specific personal account / identity for that purpose using their work email address, rather than using a personal social media account.

Staff members must not have contact through any personal social medium with any student whether from Aldridge Education or any other school, unless the student(s) is / are family members.

Aldridge Education does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

If staff members wish to communicate with students through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7 and Appendix A.

Staff members must decline 'friend requests' from students they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official school site.

On leaving Aldridge Education service, staff members must not contact Aldridge Education pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, Trust staff and other parties and school or Trust corporate information must not be discussed on their personal web space.

Photographs, videos or any other types of images of pupils and their families or images depicting staff members wearing school or Trust uniforms or clothing with school or Trust logos or images identifying sensitive school or Trust premises must not be published on personal web space.

School or Trust email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Aldridge Education or Trust corporate, service or team logos or brands must not be used or published on personal web space without the authorisation of the Director of Marketing and Communications.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection (Principal – DSL)

Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

Staff should not use personal social media, email accounts or mobile phones to contact members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Principal.

Aldridge Education does not permit the use of personal social media whilst at work using school equipment.

8. Monitoring of internet activities

Aldridge Education monitors usage of its Internet and email services without prior notification or authorisation from users.

Users of Aldridge Education cloud services, email and Internet services should have no expectation of privacy in anything they create, store, send or receive using the school's IT systems.

9. Breaches of policy

All staff are required to adhere to this policy. Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Aldridge Education Disciplinary Policies and Procedures.

A breach of this policy leading to breaches of confidentiality, defamation, damage, or illegal acts to the reputation of Aldridge Education Trust, schools or organisations as well as any acts that render Aldridge Education liable to third parties.

Contracted providers of Aldridge Education service must inform the relevant school or Trust senior team immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the Trust. Any action against breaches should be according to contractors' internal disciplinary procedures.

The member of staff will be expected to co-operate with the school's investigation which may involve:

- handing over relevant passwords and login details;
- printing a copy or obtaining a screenshot of the alleged unacceptable content;
- determining that the responsibility or source of the content was in fact the member of staff.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school/trust or the individuals concerned. Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the Trust disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee. Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

APPENDIX A

Requirements for creating social media sites on behalf of Aldridge Education

A.1 CREATION OF SITES

A.1.1 Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Aldridge Education service.

A.1.2 Prior to creating a site, careful consideration must be given to the purposes for using social media, whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome. and whether those purposes require a new site to be created rather than participation on an existing site / account. Social media communication works most effectively where there are already high numbers of followers / viewers and where content is kept fresh and constantly evolving. The assumption should always be on posting content to existing school or Trust accounts rather than creating new ones, using tagging where appropriate to encourage conversations around specific topics or audiences.

A.1.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the Director of IT or Director of Marketing.

A.1.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

A.1.5 The Principal of relevant managers must take overall responsibility to ensure that enough resources are provided to keep the site monitored, refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

A.1.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the Trust's brand and image.

A.1.7 A central register of school / Trust web and social media accounts, including the email address connected with that account, will be maintained by the local IT manager. It is the responsibility of the line manager authorising the creation of the account to ensure that the details are passed to their local IT manager. This prevents issues of schools being unable to access or close old accounts created by someone who has left and login details have been lost / not recorded. When a member of staff leaves, it is the responsibility of their line manger to ensure that the account is transferred to an email address of a continuing member of staff or closed down, and the local IT manager notified immediately.

A.1.8 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

A.2 CHILDREN AND YOUNG PEOPLE

A.2.1 When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

A.2.2 When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online ‘friends’ as real friends, be targets for ‘grooming’ or become victims of cyberbullying.

A.2.3 If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

A.2.4 Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008).

A.2.5 Staff members must also ensure that the web space they create on third party sites comply with the site owner’s minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

A.2.6 Care must be taken to ensure that content is suitable for the target age group and contributors or ‘friends’ to the site are vetted.

A.2.7 Careful thought must be given to the profile of young people when considering creating sites for them. For example, the Internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school or the Trust. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your Director of IT or Director of Marketing (or appropriate manager).

A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

A.3.1 Aldridge Education social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Aldridge Education employees or other authorised people.

A.3.2 Approval for *creation* of sites for work purposes, whether hosted by the school, Trust or hosted by a third party such as a social networking site, must be obtained from the staff member’s line manager and the Trust Director of IT or Director of Marketing in accordance to the Trust Social Media approval process.

A.3.3 Approval for *participating*, on behalf of Aldridge Education, on sites created by third parties must be obtained from the staff member’s line manager, the Trust’s Director of IT or Director of Marketing.

A.3.4 *Content* contributed to third-party hosted sites must be discussed with and approved by the staff member’s line manager and the Director of IT or Director of Marketing

A.3.5 The Trust’s Director of IT or Director of Marketing must be consulted about the purpose of the proposed site and its content. In addition, the Director of IT or Director of Marketing approval must be obtained for the use of the school logo and brand.

A.3.6 Staff must complete the Social Media Site Creation Approval Form (Appendix B).

A.3.7 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Director of Marketing and Communications immediately. Staff members must not communicate with the media without the advice or approval of the Director of Marketing and Communications.

A.4 CONTENT OF WEB SPACE

A.4.1 Aldridge Education hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school or Trust standards of professional conduct and service.

A.4.2 Trust and school web sites and social media accounts exist to contribute to the promotion of the school and / or Trust. School users should ensure they are aware of the key messages the Principal has agreed and ensure content supports and promotes these messages. Line managers should monitor that this is being done effectively. Similarly, for the Trust, all content should support the key messages in the Marketing Strategy.

A.4 3 Staff members must not disclose information, make commitments or engage in activities on behalf of Aldridge Education or the Trust without authorisation.

A.4.4 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the Trust's or Trust's image, reputation and services.

A.4.5 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

A.4.6 It is the responsibility of the member of staff posting on a web site or social media to ensure that they have permissions to use any third-party materials, including pictures, screen grabs and text. Images downloaded from the web may be subject to copyright and usage charges, and should not be used unless the user has ascertained the they are not subject to any charges or breach of copyright by so doing, or that those charges have been paid in advance of use. In terms of content it is better policy to link to another appropriate site than to copy and paste content from it.

A.4.7 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

A.4.8 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

A.4.9 Aldridge Education hosted sites must always include the up to date school logo to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.

A.4.10 Schools' websites must also carry the Aldridge Education logo and approved text about the Trust as a page within the About Us (or similar) section. The Director of Marketing and Communications can provide these resources.

A.4.11 Staff members participating in Aldridge Education hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.

A.4.12 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

A.4.13 Personal opinions should not be expressed on official sites.

A.5 CONTRIBUTORS AND MODERATION OF CONTENT

A.5.1 Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

A.5.2 Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.

A.5.3 The content and postings in Aldridge Education -hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site. Moderation responsibility includes at least daily monitoring of any contact through the site, and swift appropriate response to it.

A.5.4 The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach our policies. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

A.5.5 For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.

A.5.6 Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

A.5.7 Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly.

A.5.8 Any proposal to use school social media to promote or recommend third parties or contributors to sites must be approved by the Principals first or if necessary refer to the Trust's Director of IT or Director of Marketing.

A.5.9 If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.

A.5.10 Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.

A.5.11 Staff are also advised to consider the reputation of the Trust in any posts or comments related to the Trust on any social media accounts.

A.5.12 There are many legitimate uses of social media within the curriculum to support student learning and to encourage an interest in learning. Some have been setup per example to promote a love for the subject and increase engagement at GCSE level. There are many possibilities for using social media to enhance and develop students' learning. Staff are advised to use these technologies safely.

A.5.13 When using social media for educational purposes, the following practices must be observed: Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and has to be linked to an official school email account.

A.5.14 Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts. Staff need to comply with Data Protection regulations and other existing Trust policies.

A.5.15 Care must be taken that any links to external sites from the account are appropriate and safe.

A.5.16 Staff should not engage with any direct messaging of students through social media where the message is not public.

A.5.17 Those managing and supervising social media sites associated with the school must monitor any requests for information about the school and its activities and if they do not feel competent to answer them fully within the remit of the site must pass them on immediately to the Principal so that they can be assessed in relation to the Trust's duties under the Freedom of Information Act.

APPENDIX B

Social Media Site Creation Approval Form – Please visit this link for the digital form (recommended version)
Use of social media on behalf of Aldridge Education must be approved prior to setting up sites.
Please complete this form and forward it to the Aldridge Education IT team as a change request.

TEAM DETAILS	
Full Name:	
Department Name:	
Name of Site/Academy/Organisation:	
PURPOSE OF SETTING UP SOCIAL MEDIA SITE (please describe why you want to set up this site and the content of the site)	
What are the aims you propose to achieve by setting up this site? Can't these be achieved through existing sites or social media channels?	
What is the proposed content of the site?	
Proposed audience for the site:	
Main supervisor:	
Reserve supervisor:	
Proposed frequency of Normal monitoring:	
Proposed frequency of monitoring during holidays:	
Person responsible for monitoring / updating the site and responding to users	
Email address linked to the site	
Published ID/Name linked to the site	

APPROVAL from relevant stakeholders below must be obtained before the site can be created. Any site created will normally be expected to be generated in conjunction with the Cluster IT Manager to ensure that access information is properly recorded and privacy and security settings adopted in accordance with Trust's policies. The relevant managers must read this form and complete the information below before final approval can be given by the Trust Director of Marketing/IT.

Head of Department: I approve the aims and content of the proposed site.		**Principal:** I approve the aims and content of the proposed site and the use of school brand and logo.	
Comments:		**Comments:**	
Name		Name	
Signature		Signature	
Director of Marketing / Director of IT:			
Signature			
Date			