CHILTERN LEARNING TRUST

SOCIAL MEDIA POLICY

Date Reviewed	Body	Next Review Date
Autumn Term 2023	Board of Trustees	Autumn Term 2024

1 Introduction

1.1 This policy provides the acceptable standards for the use of social-media platforms for all employees at Chiltern Learning Trust. Volunteers and casual workers should also be made aware of the standards and expectations set out in this policy.

1.2 This policy should be read in conjunction with Working Together to Safeguard Children Framework, Keeping Children Safe in Education (September 2023), the Code of Conduct, the Internet and E-mail and Acceptable Use Policy and the Social Media Policy

1.3 For the purposes of this policy, social media is any online platform or any application that allows parties to communicate instantly with each other or to share data in a public forum. This includes social media forums such as X, Facebook, Instagram, Snapchat, LinkedIn and Reddit. Social media also covers blogs, and video / image-sharing websites such as Youtube. It further covers gaming platforms (such as Minecraft, World of Warcraft etc), online discussion groups, dating sites, and gambling sites. It also covers other forms of electronic communication software/applications such as texting, SMS, WhatsApp, and Facebook Messenger.

Employees should be aware that there are many more examples of social media than can be listed here and it is a constantly changing area, therefore, the examples listed are not an exhaustive list. Employees should follow these guidelines in relation to any social media that they use.

1.4 The Trust understands that many people may choose to use social media sites/applications in their private lives. This policy does not seek to prevent the use of social media sites/applications, but seeks to provide clear guidelines on the acceptable use of social media by employees.

2 Communications

2.1 There are two different forms of communication: personal communications and professional communications.

2.2 Personal communications are those made via a personal social media account. Personal communications that demonstrate a failure to follow professional standards or could damage the Trust reputation are within the scope of this policy.

2.3 Professional communications are those made through official channels, posted on a school social media account, or using the Trust name. All professional communications are within the scope of this policy.

3 Purpose

3.1 The purpose of this policy is to:

- Set out clear guidance on the acceptable use of social media sites/applications
- Safeguard children
- Ensure confidentiality of the school, its employees and pupils is maintained at all times
- To protect the reputation of the Trust

- Ensure that all employees understand the consequences of failing to comply with the social Media Policy
- Ensure the appropriate use of the Trust's resources

4. Local Governing Body/Headteacher responsibilities

4.1 Luton HR Traded Services will provide guidance on updating this policy as and when appropriate.

4.2 It is the responsibility of the Headteacher to publicise and make this policy available to all, ensuring that the standards within it are both monitored and enforced, and to advise the Local Governing Body of any serious breaches of this policy. It is the responsibility of the Chief Executive Officer (CEO) to make centrally employed staff aware of the policy.

4.3 It is the responsibility of the Local Governing Body, Headteacher to take corrective and/or disciplinary measures as are necessary when a breach of this standard occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards may constitute a criminal act.

5 Employees' responsibilities

5.1 It is the responsibility of the employee, volunteer, or casual worker to read and comply with the Social Media Policy. Any failure to abide by the Social Media Policy may result in disciplinary action.

5.2 Employees, volunteers and casual workers **must** alert the Headteacher or a relevant senior member of staff where a breach of the policy, by themselves or another employee, is suspected or known to have occurred. Failure to do so may result in disciplinary action being taken.

5.3 **Trust employees must be aware that everything posted online is public in nature, even with the strictest privacy settings. Once something is online, it can be copied and redistributed. Therefore, it should be assumed that everything that is written online is permanent and could be shared. All information posted online is subject to Copyright, General Data Protection Regulation legislation and the Safeguarding Vulnerable Groups Act 2006**

5.4 All employees are reminded that they are bound by the Trust's Code of Conduct, and teaching staff are further subject to the Teachers' Standards. Under the Safeguarding Vulnerable Groups Act 2006 school employees may be referred to the Disclosure and Barring Service (DBS) where the Trust has significant concerns or suspicions about an employee's conduct or behaviour.

5.5 All employees are responsible for any content displayed/shared/posted on their social media accounts/applications, and as such must ensure that their privacy settings are updated and maintained appropriately and passwords are kept secure and confidential.

5.6 Trust employees, volunteers and casual workers should at all times:

- Have the highest standards of personal conduct (inside and outside of Trust)

- Ensure that their behaviour (inside and outside of Trust) does not compromise their position within the Trust
- Ensure that their judgment and integrity should not be able to be brought into question.
- Ensure that their relationship with members of the community, via social media, does not compromise their position within the Trust or bring into question their suitability to work with children and young people.

6 Safeguarding Children

6.1 Communication between children and adults, by whatever method, should take place within clear professional boundaries. Employees must abide by the agreed method of communication policies within the Trust. Adults should ensure that all communications are transparent and open to scrutiny.

6.2 Safeguarding children is the responsibility of all Trust employees, volunteers, and casual workers. The key principles that must be followed are:

- Trust employees **must not** communicate with (including accepting 'friend'/follow requests) any current pupils of the school, or from any other educational establishment, on social media sites/applications such as Facebook, Instagram etc. This is applicable **even if** there is permission from a pupil's parent/guardian. (This would not apply to school aged pupils that an individual employee is directly related to, e.g. their child, niece or nephew). Employees should alert the Headteacher if they receive any such communication from pupils.
- Employees should not communicate with, including accepting 'friend'/follow requests from, past pupils whilst they are below the age of nineteen. Employees should alert the Headteacher if they receive any such communication form past pupils.
- Employees should ensure that all their social media account settings require them to authorise or accept people as friends or followers to avoid this occurring without their knowledge or approval.

6.3 These principles apply:

- Regardless of whether access occurs during or outside of contracted work hours.
- To all technology or devices whether provided by the school, or personally owned.

7 Unacceptable use of Social Media Sites/Applications

7.1 Through Social Media Sites/Applications, employees **must not**:

- Disclose private and/or confidential information relating to pupils, parents, other Trust employees, their employment directly, or the Trust. This also applies to any other educational establishment that the employee has worked within.
- Discuss or reveal any matters relating to the Trust, previous educational establishments, Trust employees, pupils or parents
- Publish, share, distribute or comment on any material that may be deemed contrary to British Values*.
- Identify themselves as a representative of the Trust online, or on their social media sites/profiles

- Write abusive comments regarding current/previous Trust employees, governors, current/previous pupils or parents/guardians
- Harass or bully current/previous Trust employees, or any persons unrelated or related to the Trust through cyber bullying and social exclusion
- View or update their personal social media account/profile (on Facebook, Twitter, Instagram, Snapchat etc) during the working day, unless on a designated break. (This includes via a work or personal mobile telephone and/or iPad).
- By proxy, update their personal social media account/profile (Facebook, Twitter, Instagram, Snapchat etc) during their normal working day, and must ensure that their social media site/application is secure at all times from third parties
- Access or share illegal material
- Publish any content, which may be deemed as defamation or discrimination
- Post any images of pupils from the Trust or any other previous education establishment where the employee has worked
- Without permission, post any images of Trust employees on social media sites/applications from the Trust or any other previous education establishment where the employee has worked.
- Set up and/or use an alias social media account to circumvent the policy
- Comment/post/share any material which could bring the school into disrepute
- Breach any of the Trust's other policies and procedures such as the Trust's Code of Conduct, Bullying and Harassment Policy, Equal Opportunities Policy
- Use social media sites/applications as a forum for raising and escalating concerns regarding the Trust. These concerns should be raised through the line manager or using the Grievance Procedure or the Whistleblowing Procedure.

  This list is not exhaustive and should be read in conjunction with the Internet and E-mail Acceptable Use Policy and the Code of Conduct.

8 Personal Use of Social Media Sites and applications

Employees, volunteers and casual workers are reminded that they are entitled to undertake private conversation on social media sites and applications. However, employees must accept that if the conversation becomes public and the content is deemed to be inappropriate and/or unprofessional disciplinary action may be undertaken.

Employees, volunteers and casual workers should ask themselves the following question "if this conversation became public knowledge could it raise questions about my integrity or suitability to work in a Trust and could it bring the Trust into disrepute?"