Social Media and Internet Acceptable Use Policy



Hillborough Infant and Nursery School

Owned and Written by: Luton Schools HR Team	**Date:** April 2026
Approved by: Full Governing Body	**Date:** April 2026
Next Review:	**Date:** When policy is updated by Luton HR Team
This policy has been updated to reflect the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and it supersedes the HM Government Information Sharing Guidance for Practitioners and Managers published in March 2015.	

Contents

1.0 Introduction 3
2.0 Communications 3
3.0 Purpose 3
4.0 Governing Body/Headteacher responsibilities 4
5.0 Employees' responsibilities 4
6.0 Safeguarding Children 5
7.0 Unacceptable use of Social Media Sites / Apps 5
8.0 Personal Use of Social Media Sites / Apps 6
9.0 Email Use 7
10.0 Internet Use 7

1.0 Introduction

1.1 This policy provides the acceptable standards for the use of social media and internet based platforms for all employees. 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 Keeping Children Safe in Education, the school's Code of Conduct and the Mobile Phone Policy/Guidelines (*if applicable to school).

1.3 For the purposes of this policy, social media is any online platform or any application or "app" that allows parties to communicate with each other or to share data in a public forum. This includes social media forums such as 'X' formerly known as Twitter, Facebook, Instagram, Snapchat, TikTok, LinkedIn and Reddit. Social media also covers blogs and video / image-sharing websites such as YouTube. In addition, it covers gaming platforms (such as Minecraft, World of Warcraft etc), online discussion groups or forums, dating sites and gambling sites.

1.4 This policy also applies to the use of other forms of communication apps such as e-mail, texts, SMS, WhatsApp, Facebook Messenger, Microsoft Teams, Google Meet and Zoom on both personal and school accounts/ devices. Employees should follow these guidelines in relation to any social media / apps that they use.

1.5 Employees should be aware that there are many more examples of social media / apps than can be listed here and it is a constantly changing area, therefore, the examples listed are not an exhaustive list. If an employee is unsure whether this policy applies to a particular app, site or other method of communication, they should seek advice from their headteacher.

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

2.0 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 or apps. Personal communications that demonstrate a failure to follow professional standards or could damage the school/ employer reputation are within the scope of this policy.

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

3.0 Purpose

3.1 The purpose of this policy is to:

- set out clear guidance on the acceptable use of social media sites/ apps

- safeguard children and young people
- ensure confidentiality of the school, its employees and pupils is maintained at all times
- protect the reputation of the school/trust
- ensure that all employees understand the consequences of failing to comply with the Social Media and Internet acceptable use Policy
- ensure the appropriate use of the school's resources

4.0 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 governing body of any serious breaches of the policy. In a Trust, 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 governing body, headteacher and/or CEO to take corrective and/or disciplinary measures as are necessary when a breach of these standards occur and to contact and co-operate with police and other law enforcement agencies where a breach of these standards may constitute a criminal or unlawful act.

5.0 Employees' responsibilities

5.1 It is the responsibility of the employee, volunteer, or casual worker to read and comply with the Social Media and Internet acceptable use Policy. Any failure to abide by this 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. Employees should ensure that they are fulfilling their responsibility in relation to filtering and monitoring by reporting any incidents of harmful or inappropriate content being accessed on school IT equipment. Failure to do so may result in disciplinary action being taken.

5.3 **School 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 or screenshotted 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 school'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 school has significant concerns or suspicions about an employee's conduct or behaviour.

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

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

- have the highest standards of personal conduct (inside and outside of school)
- ensure that their behaviour (inside and outside of school) does not compromise their position within the school
- 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, email or the internet, does not compromise their position within the school or bring into question their suitability to work with children and young people

6.0 Safeguarding Children

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

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

- School employees **must not** communicate with (including accepting 'friend'/ follow requests where the site provides this option) any current pupils of the school, or from any other educational establishment, on social media sites/apps such as Facebook, Instagram or communicate with them via personal email or internet accounts. This is applicable **even if** there is permission from a young person'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 or a close family friend). 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 from past pupils.
- Employees should ensure that all their social media or internet accounts / app settings require them to authorise or accept people as friends or followers, where the site allows, 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

7.0 Unacceptable use of Social Media Sites / Apps

7.1 On Social Media sites or apps, employees **must not**:

- disclose private and/or confidential information relating to pupils, parents, carers, other school employees, their employment directly, or the school. This also applies to any other educational establishment that the employee has worked with or within.

- discuss or reveal any matters relating to the school, previous educational establishments, school 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 school online, or on their social media sites/profiles
- write abusive comments regarding current/previous school employees, governors, current/previous pupils or parents/guardians
- harass or bully current/previous school employees, or any persons unrelated or related to the school 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 phone and/or iPad).
- ensure that where their account is updated by proxy, it remains in line with the guidance in this policy. Any employees whose account is legitimately managed by a third party, such as a political party or charity, is advised to share this policy and speak to the headteacher if they have any concerns
- access or share illegal material
- publish any content, which may be deemed as defamation or discrimination
- post any images of pupils from the school or any other previous education establishment where the employee has worked
- without permission, post any images on social media sites/apps of school employees or images from the school 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 school's other policies and procedures such as the school's Code of Conduct, Bullying and Harassment Policy, Equal Opportunities Policy
- use social media sites/ apps as a forum for raising and escalating concerns regarding the school/Trust /academy or the Council. 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 Code of Conduct.

8.0 Personal Use of Social Media Sites / Apps

8.1 Employees, volunteers and casual workers are reminded that they are entitled to undertake private conversations on social media sites /apps. 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.

8.2 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 school and could it bring the school into disrepute?"

9.0 Email Use

9.1. Employees are provided with a school email account and should only use this email account for professional, school related email communication with parents/carers, students and colleagues. All email communication should be traceable in the school's email system.

9.2 Email accounts are provided for business use. Therefore, the content of all emails should at all times remain professional and be related to work matters.

9.3 Under no circumstances should employees, volunteers or casual workers contact or engage with pupils, parents or conduct any school business using a personal email address.

9.4 Emails should never be sent, forwarded or replied to where the content is adult, explicit, offensive or otherwise inappropriate. Any emails received containing such content must be reported to the headteacher.

Inappropriate email content includes, but is not limited, to: ● violent or threatening emails

- abusive/obscene/discriminatory/offensive language
- emails that could be construed as bullying
- defamatory comments about the school/academy/trust or colleagues
- emails with content potentially harmful to the school/Trust/Academy/Council
- emails that could be construed as harassment
- insulting or offensive emails
- emails containing sexual innuendos or content
- politically biased emails
- content contrary to the school ethos

10.0 Internet Use

10.1 Websites, web searches and internet pages that are visited during working hours should be related to school or workplace matters. However, on occasion, access to websites unrelated to school business may be permitted at the discretion of the headteacher during designated break periods.

10.2 Employees must not access sites on school owned devices which contain inappropriate material such as, but not limited to:

- Adult, explicit, or offensive content including any such jokes, pictures or profanity (including images or other searches for such material)
- Incitement of violence, disorder, racial or other discriminatory hate or ideologies ● Radicalisation or the promotion of terrorism
- Chat rooms
- Personal ads or dating sites
- Criminal skills or resources, e.g. hacking, virus writing or password cracking
- Illegal drugs, gambling, violence or weapons
- Downloads of games. (except for downloads authorised by the school and in compliance with copyright law).

10.3 Employees must not show any inappropriate websites/pages, videos, images or any other online content, on any internet enabled device to pupils. Employees should seek clarity from the headteacher on the appropriateness, including any relevant age restrictions, of the online content if they are unsure.

10.4 Employees, volunteers or casual workers should always preview any websites/pages or online services before using them in lessons or with pupils or parents.

10.5 Searching for images or videos through open search engines is discouraged when working with pupils.

10.6 In compliance with the Information Commissioner's Office Employment Practices Code you are advised that the School / Trust / Academy or their agents will monitor, and may investigate, access to the internet, social media, apps and use of email and school computer equipment to ensure compliance with this policy.