Social Media Policy and Guidance

Policy Level	Trust	Ref No	ADM05
Approved by	Executive Team	Approved date	12.01.2026
Responsibility	Deputy CEO	Next review	Spring 2028
Reviewed by	V Gavin	Date Issued	Spring 2026

Document Control	
Title	Social Media Policy and Guidance
Date	December 2025
Supersedes	Social Media Policy and Guidance 2022
Amendments	3.4 Including Mobile Phones 6.4 All such requests should be notified to the headteacher and the Deputy CEO. 6.7 All requests should be rejected and reported to the Headteacher or Deputy CEO. 6.10 The Trust advises staff not to engage in social networking with former pupils. However, if an employee chooses to connect with a past pupil, this should only occur after a reasonable amount of time has passed since they left the school—for example, once the individual has reached the age of 21. 8.2 Trust social media accounts list updated Throughout Director of Academy Operations changed to Deputy CEO, and the Academy Lead changed to headteacher.
Related Policies/Guidance	• Safeguarding Policy • Acceptable Use of ICT Policy • Code of Conduct • Disciplinary & Dismissal Policy • Grievance, Bullying and Harassment Policy • Data Protection Policy • Equality Policy.

Contents

1 Introduction

1.1. This model policy and guidance document recognises that new technologies are an integral and growing part of everyday life and that they make an important contribution to teaching and learning opportunities in school. This policy also recognises that, in the light of the rapid evolution of social networking technologies, Bolton Impact Trust requires a robust policy framework so that all adults working across Bolton Impact Trust are aware of the expectations and the rules they are expected to follow when using social media both inside and outside of the school environment.

1.2. This policy is designed to ensure that all adults use social media responsibly in order to safeguard the trust, each school, its pupils, staff, Governors, Trustee's and members of the wider school communities. It is crucial that children are safeguarded and that parents, pupils and the public at large have confidence in the trust and its schools' decisions and services. Responsible use of social media will ensure that the confidentiality and privacy of pupils and members of staff are maintained and that the reputation and integrity of the trust and each of its Schools are protected.

1.3. This policy should be read in conjunction with other relevant school policies, in particular, the Trust/School *Safeguarding Policy**,** Acceptable Use of ICT Policy, Code of Conduct, Disciplinary & Dismissal Policy, Grievance, Bullying and Harassment Policy, Data Protection Policy and Equality Policy.*

1.4. This policy takes into account the provisions of the DfE's statutory guidance Keeping Children Safe in Education, the non-statutory guidance on Safer Working Practices with Children and Vulnerable Young Adults (May 2019) Addendum updated (April 2020), the non-statutory guidance on the Prevent Duty (April 2019), and the Briefing Note to schools on "How Social Media is used to encourage travel to Syria and Iraq". It also takes into account the Government's statutory guidance issued under s29 of the Counter - Terrorism and Security Act 2015 (June 2015).

2 Scope and definitions

2.1 This policy applies to all employees at Bolton Impact Trust and those who provide services for or on behalf of the trust or its individual Schools. This includes trainee teachers and any other trainees, apprentices, self-employed staff, agency staff, external consultants and volunteers. This policy also applies to school governors, trustees and members.

2.2 This policy covers the **personal** use of social media as well as the use of social media for **school or trust purposes** (whether official or not), including the use of websites hosted and maintained on behalf of the trust and its Schools. It covers communication through web-based and telecommunication interactions, and includes the use of computers, tablets, phones, digital cameras, videos, web-cams and other hand-held devices.

2.3 This policy covers the use of social media as defined in paragraph 3 of this policy, and also personal blogs and any posts made on other people's blogs, and all online forums and notice boards. The guidance, rules and principles set out in this policy must be followed irrespective of the social media platform or medium.

2.4 In this policy, the following definitions apply:

- **Social media** - means any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Social media includes but is not limited to online social forums such as Twitter, Facebook, Instagram, Tik Tok and LinkedIn and also covers blogs, chat rooms, forums, podcasts and video-image-sharing websites such as YouTube, Flickr, Reddit, Instagram, Snapchat, WhatsApp, Pinterest and Tumblr. The internet is a fast-moving technology, and it is impossible to cover all examples of emerging social media in this policy.
- **Adults/adults working in school** - means all members of staff and those who work on a self-employed basis. It also includes trainee teachers, other trainees and apprentices, volunteers, agency staff, external consultants and school governors, trustees and members.
- **Information** - means all types of information, including but not limited to, facts, data, comments, audio, video, photographs, images, texts, e-mails, instant messages and any other form of online interaction.
- **Inappropriate information** - means information as defined above which any reasonable person would consider to be unsuitable or that brings into question the professional integrity of the adult, given their position within the trust or its Schools.
- **the school and the wider school community** – means the trust, its Schools, its pupils, all adults working in school (as defined above), parents/carers of pupils, former pupils, and any other person or body directly or indirectly connected with the ***trust or its Schools***

3 Key Principles

3.1 Safeguarding and promoting the welfare of children is everyone's responsibility.

3.2 Adults have an important role to play in equipping the school's pupils to stay safe online, both in school and outside of school. Adults, therefore, need to be aware of the risks associated with the use of social media and in particular, about the provision and sharing of information in the social media arena.

3.3 Adults must not, whether deliberately or inadvertently and whether in their working time or in their personal time, provide, publish or share inappropriate information on or via any social media platform or medium about themselves, the trust or its schools or the wider school community.

3.4 Adults are accountable for and must take responsibility for all information published or shared by them on social media websites and for any views expressed by them on any such sites, whether in their working time or in their personal time and which may come into the public domain. Adults should be aware that their use of social media and any information published by them may be monitored by the Headteacher or Central Leadership Team, and/or members of the school's Governing Body or Trust Board. By using the school's IT resources and facilities, including mobile phones, adults give their consent for the trust to monitor their activities.

3.5 All adults who provide, publish or share information which causes harm or distress or which has the potential to cause harm or distress or to cause reputational damage to the trust, its Schools or the wider school community will be dealt with as appropriate by the Headteacher or Central Leadership Team in accordance with the relevant trust/School policy/procedure. This may include action being taken under the school's Safeguarding

Policy (which could lead to a referral to the Local Authority and/or the police), and it could also lead to disciplinary action being taken under the trust's Disciplinary and Dismissals Policy, which, in serious cases, may lead to dismissal without notice.

3.6 The principles which underpin this policy are: -

- adults are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions;
- adults must be conscious at all times of the need to keep their personal and professional lives separate; adults must not put themselves in a position where there is a conflict between their work and personal interests;
- adults must work and be seen to work, in an open and transparent way;
- adults must continually monitor and review their own practices in terms of the continually evolving world of social networking and social media and ensure that they consistently follow the rules, principles and guidance contained in this policy.

4 Rules and Responsibilities

4.1 The Trust Board, Local Governing Bodies, Headteachers, and Central Leadership Team will:

- ensure that all adults working at the trust are familiar with this policy and any related policies;
- take all reasonable steps to enable adults working with children to work safely and responsibly and to support safer working practice in general with regard to the use of the internet and other communication technologies;
- ensure appropriate filters and monitoring systems are in place;
- take all reasonable steps to assist adults to monitor their own practices and standards with regard to the use of the internet and other communication technologies;
- set clear rules in relation to the expected standards of behaviour relevant to social networking for educational, personal, or recreational use;
- give a clear message that unlawful or unsafe behaviour or practice is unacceptable and that, where appropriate, disciplinary, legal and/or other action will be taken;
- ensure that all concerns raised in relation to accessing social media or social networking sites are investigated promptly and appropriately;
- ensure procedures are in place to handle allegations against any adult;
- take all reasonable steps to minimise the risk of misplaced or malicious allegations being made against all adults working across the trust;
- take all reasonable steps to prevent adults working across the trust or within the schools from abusing or misusing their position of trust.

4.2 Adults working at The Bolton Impact Trust must: -

- ensure they are familiar with the contents of this policy;
- adhere to and apply the rules, guidance and principles in this policy in all aspects of their work and in their personal time;
- act in accordance with their duties and responsibilities under this policy and the statutory/ non-statutory advice and guidance referred to;

- raise any concerns or queries in connection with this policy with the Headteacher or Deputy CEO;
- notify the Headteacher or Deputy CEO of any inappropriate posts on social media forums by a colleague, parent or pupil which have the potential to bring the school into disrepute;
- attend any training provided or facilitated by the trust or its schools in relation to the use of the internet or any other communication technologies;
- never, in any circumstances, abuse or misuse their position of trust.

5 Safer social networking practice

5.1 Adults must be aware of the risks and dangers of revealing personal information on social networking sites. Disclosing personal information on social networking sites may compromise an adult's personal safety and security, and it also increases the potential for pupils, their families or friends to have access to adults outside of the school environment. Personal information as defined by the General Data Protection Regulations (2018) is considered as any information about an individual that would identify them, and includes information such as a home address, home and mobile telephone numbers and details relating to the place of work.

5.2 Adults, particularly those new to the school setting, must review their social networking sites when they join the trust or its Schools and should ensure that they have the appropriate privacy settings in place to ensure that information available publicly about them is appropriate and accurate. This should include reviewing any photographs or images that may cause embarrassment to them and/or to the trust, its schools and the wider school community. **See Appendix One for guidance on Facebook use.**

5.3 It is the adult's responsibility to ensure they are familiar with the school's IT policies, including the school's Acceptable Use policy, and to seek school guidance should they be unsure about privacy settings, online activity and/or information sharing on their personal social media accounts.

5.4 It is the adult's responsibility to ensure all their social media accounts are reviewed regularly and that the appropriate privacy settings remain in place to ensure their information is not open to the public domain.

6 Responsibilities when using social media

6.1 Adults must take responsibility for their personal telephones and any personal electronic devices and must keep their personal telephone numbers, login details, passwords, PIN details and personal email addresses private and secure.

6.2 Where there is a need to contact pupils or parents, the school's email address and/or telephone number should be used. Adults must not use their personal telephones or email accounts for these purposes.

6.3 Adults must understand who is allowed to view the content on their social media pages of any websites they use and how to restrict access to certain groups of people. Appropriate privacy settings are vital.

6.4 Adults must not request, or respond to a request for any personal information from or about a pupil at the trust or one of its schools. All such requests should be notified to the headteacher and the Deputy CEO.

6.5 Adults must not engage in conversations about pupils with their parents or carers or with any other person by any form of social networking or social media unless they have the express permission of the Headteacher or Deputy CEO to do so.

6.6 Adults must only use the official school emails or school phones for communicating with pupils/parents. Any communications with pupils/parents (including by email, telephone or text communications) outside of agreed protocols will be treated as a very serious conduct matter and may lead to disciplinary action being taken under the trust's Disciplinary Policy, which, in serious cases, may lead to dismissal without notice. It may also lead to a criminal investigation.

6.7 Adults must never connect to or have any contact with a pupil from any of the trust schools on any social networking site. The only exceptions to this rule are where the pupil is a member of the adult's family, provided agreed protocols are followed and the family relationship has been identified to and acknowledged by the Headteacher/Deputy CEO. All requests should be rejected and reported to the Headteacher or Deputy CEO.

6.8 In cases where a pupil is a family member, adults must be aware that if the family relationship has not been identified and acknowledged by the trust, contact through social networking or social media will be a breach of this policy (and therefore will be treated as a serious conduct issue). Adults must be clear that such contact could also be misconstrued as being part of a grooming process. Since family relationships can be easily identified and recognised, adults must notify their Headteacher of any family relationship with a pupil so that the position can be formally acknowledged, discussed and recorded.

6.9 Adults must never use or access the social networking sites or social networking pages of pupils from schools within the trust unless the pupil is a member of the adult's family and the family relationship has been acknowledged and discussed in advance with the Headteacher.

6.10 Adults must be cautious about any form of social networking contact with former pupils, parents/carers of pupils, particularly where siblings or other relatives continue to attend the school or may attend the school in future. The Trust advises staff not to engage in social networking with former pupils. However, if an employee chooses to connect with a past pupil, this should only occur after a reasonable amount of time has passed since they left the school—for example, once the individual has reached the age of 21.

6.11 Adults must be mindful at all times of the boundaries between their work and personal life in accordance with the Key Principles detailed in this policy, and in the Guidance for Safer Working Practices for Adults who work with Children and Young People in Education 2019 Addendum updated April 2020.

6.12 Adults must also be cautious when inviting work colleagues to be friends on social networking sites. Social networking sites can blur the boundaries between work and personal lives, and it may be difficult to maintain professional relationships.

6.13 Adults must not use social media and the internet in any way to attack, insult, criticise, abuse or defame pupils, family members of pupils, colleagues, Headteachers, The Trust

Central Team, Trustees, Governors, the trust or Schools in general and the wider school community. Adults must always show respect to others when using social media.

6.14 Adults must never post derogatory remarks or offensive comments online or engage in online activities which may bring them, the trust, its Schools or the wider school community into disrepute or which could be interpreted as reflecting negatively on their professionalism.

6.15 Adults must not represent their personal views on any social media forum as being in any way linked to the trust, its Schools or being the views of the trust.

6.16 Photographs, videos or any other types of images of pupils and their families or images depicting staff members or where the schools or the trust can be identified, must not be published on social media.

6.17 Where social networking and other web-based sites have fields in the user profile relating to job title or information, all adults should not put any information onto the site which could identify the trust/schools or their role at the trust (particularly teachers and teaching assistants where pupils may be identifiable). In some circumstances, the provision of such information could damage the reputation of the trust or its Schools and/or the relevant profession.

6.18 Teachers must at all times be mindful of the Teachers' Standards applicable to their profession and act in accordance with those standards. The Teacher Standards make clear that a teacher must uphold public trust in the profession and maintain high standards of ethics and behaviour both within and outside of school, by ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law. Any breach of the Teacher Standards will be considered a matter of misconduct and may lead to disciplinary action being taken under the trust's Disciplinary and Dismissals Policy, which, in serious cases, may lead to dismissal without notice.

6.19 Adults must devote the whole of their time and attention to their duties during working hours. Personal use of the internet is not permitted during working hours, and it is strongly recommended that 3G/4G access is switched off during working hours. Exceptions to this must be agreed by a member of the school leadership team (SLT) and reviewed regularly. Any breach of this provision will be regarded as a conduct matter and disciplinary action will be taken as appropriate. We understand that some staff have mobile phones for work purposes; however, these should not be used in classrooms or during contact time with pupils and should be placed on silent during these times if unable to turn them off. Social media sites must only be used during working hours for purposes of posting on official trust social media sites relating to school activities. Wherever possible, this should be done at the start or the end of the day outside of core pupil contact hours.

6.20 Confidentiality issues must be considered at all times in relation to social networking and the use of social media. All employees are bound by a common law duty of fidelity. There are also other laws which protect the trust's confidential information, which adults working in schools may have access to during the course of their work. Confidential information includes but is not limited to person identifiable information, for example pupil and employee records, information protected by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018 and information provided by the school in the expectation of confidence including information about the trust, its Schools, pupils and the families of pupils, the trust/Schools staffing or business plans, and any other commercially or politically sensitive information.

6.21 Adults must ensure that they do not provide, publish share or otherwise disclose any confidential information about themselves or about the trust or its Schools and the wider school community in breach of their duty of fidelity or in breach of other laws relating to confidentiality and privacy including the Human Rights Act 1998, the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018.

6.22 Adults must ensure they understand their obligations under the Equality Act 2010 and under the Trust's Equality Policy. Breaches of the Equality Act 2010 or the trust's Equality Policy through the use of social networking or social media will be considered a serious conduct matter which may lead to disciplinary action being taken under the trust's Disciplinary and Dismissals Policy, which, in serious cases, may lead to dismissal without notice. Adults should also be aware that they could be held personally liable for their own discriminatory actions under the Equality Act 2010. If, for example, an adult was to harass a co-worker online or engage in a discriminatory act in relation to one of the protected characteristics under the Equality Act 2010, this may result in legal action being taken against them.

6.23 Adults should also be aware that there are other laws relating to libel, defamation, harassment and copyright which may apply to information, published or posted by them on social media, and which could lead to legal action being taken against them. In addition, this will be considered as a serious conduct matter and may lead to disciplinary action being taken in line with the trust's Disciplinary Policy, which may lead to dismissal without notice.

6.24 All concerns about communications, social contact or social media/social networking issues must be raised with the Headteacher or Deputy CEO immediately.

7 Access to inappropriate images

7.1 There are no circumstances which justify adults possessing or sharing indecent images of children, whether in working time or in an adult's personal time. Adults who access and/or possess links to such material or websites will be viewed as a significant and potential threat of harm to children or vulnerable adults. Appropriate action will be taken against the adult concerned in these circumstances, which, for the avoidance of doubt, could include action under the Safeguarding Policy (which could lead to police and Local Authority involvement) and disciplinary action under the trust's Disciplinary and Dismissals Policy (which could result in dismissal without notice on the grounds of gross misconduct). Where indecent images of children are found by any adult, the Deputy CEO must be informed immediately.

7.2 Adults must not use equipment belonging to the school to access pornography or adult or explicit material of any kind. Personal equipment containing these images or links to them must not be brought into school. If any adult uses school equipment or personal equipment in school to access pornography or links to it, this will raise serious concerns about the suitability of the adult concerned to work with children. This will lead to an investigation under the trust's Disciplinary and Dismissals Policy and may lead to disciplinary action and any other action considered appropriate in the circumstances.

7.3 Adults must ensure that pupils are not exposed to any inappropriate information, images or web links. The trust and its Schools will endeavour to ensure that internet equipment used by pupils has the appropriate controls with regard to access. Any concerns or potential issues identified by any adult must be reported immediately to the Headteacher or Deputy CEO.

7.4 Where any form of unsuitable material is found, which may not be illegal, but which could or does raise concerns about an adult working in school, the Headteacher should be informed immediately. The Headteacher may take HR or legal advice on the appropriate way forward.

8 School social media websites

8.1 There must be a strong pedagogical or business reason for creating an official school social media page, social networking website, including professional WhatsApp groups or other social networking groups, and websites to communicate with pupils and parents/carers. Adults must not create social media pages, websites or groups for reasons which could expose the trust or its Schools to unwelcome publicity or which could cause reputational damage to the Trust. The matter must have been discussed, authorised and agreed with the Headteacher and Deputy CEO in advance of the creation of any school website, including social media pages and social networking groups, being created. The use of these forums must be reviewed and maintained regularly to ensure contact is in accordance with the agreed protocol.

8.2 The Trust has a number of official social media pages. Only the social media pages detailed below should be used for any post relating to the schools, pupils or the trust. The designated staff for each social media page is listed below, and they are responsible for ensuring all posts are:

- professional
- reflective of trust and the school's image
- in line with GDPR guidelines
- subject to the appropriate consent
- Celebratory

Staff members who have not been authorised to manage or post to the account must not access or attempt to access the account. Trust/School accounts must be approved before set-up using the request form at Appendix 1, and account holders must agree to follow the trust guidelines, which can be found at Appendix 2

School	Social media pages	Managed by/Posts by
Park School	Facebook	K. Heyes
Lever Park	Facebook (Therapy Farm)	O. Fay
Smithills School	Facebook	R. Abbott/ M. Khan
	Instagram	
	You Tube	

8.3 Adults must not have personal social media pages which reference any of the schools or the trust unless it has been approved by the Headteacher and Deputy CEO. Adults must not post any pictures or content relating to any of its Schools or the trust on any personal social media sites; failure to comply with this could result in the application of the trust's disciplinary and dismissal policy.

8.4 Adults must at all times act in the best interests of the trust and its Schools and the pupils when creating, participating in or contributing to the content of any website or social media site created on behalf of the trust or its Schools.

9 Cyberbullying and Trolling

9.1 '**Cyberbullying'** 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.'

9.2 If cyberbullying takes place, adults should keep records of the abuse, texts, e-mails, website or instant messages and should not delete the said texts, e-mails or messages. Adults are advised to take screen prints or 'screenshots' of messages or web pages and to be careful to record the time, date and location of the site.

9.3 **'Trolling'** can be defined as 'circumstances where a person sows' discord online, starting arguments or upsetting people by posting inflammatory, insulting or threatening messages with the deliberate intent of provoking an emotional response.'

9.4 If trolling occurs, adults are advised to take screen prints or 'screenshots' of messages and should not delete any evidence of trolling.

9.5 Adults must report all incidents of cyberbullying and/or trolling to the Headteacher and Deputy CEO. Any such incidents will be taken very seriously. Adults who have been subjected to cyberbullying or trolling may wish to seek the support of their trade union or professional association representative.

10 The Prevent Duty

10.1 Schools have a vital role to play in equipping children and young people to stay safe online, both in and outside school and also in protecting pupils from the risks of extremism and radicalisation. Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on specified authorities (including schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism (the Prevent Duty).

10.2 Terrorist organisations, such as ISIS, are attempting to radicalise and recruit young people through extensive use of social media and the internet. As with any other online risks of harm, every adult in school (teachers and teaching assistants in particular) must be aware of the risks posed by the online activity of extremist and terrorist groups.

10.3 The Government has issued statutory guidance in relation to the Prevent Duty (June 2015). In addition, to assist schools and to help recipients understand the implications of the duty, the DfE has also produced non-statutory advice (June 2015). Adults should familiarise themselves with the guidance and the advice, both of which are available in the school office/on the school website.

10.4 The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school will ensure that suitable filtering is in place. Internet safety is integral to the school's ICT curriculum, and the trust will ensure it is embedded in the school curriculum. In addition to advice on internet safety provided by the school, further general advice and resources for schools on internet safety are available on the UK Safer Internet Centre website.

10.5 Keeping children safe from risks posed by terrorist exploitation of social media should be approached by adults in school in the same way as safeguarding children from any other form of online abuse. All staff must complete prevent training every 2 years, and like with any other safeguarding issue, concerns should be raised with your School DSL or

Headteacher. The DSL will be responsible for updating staff on information regarding the prevent duty.

10.6 For the avoidance of doubt, if any adult working at Bolton Impact Trust has a concern that a particular pupil or group of pupils is at risk of radicalisation or terrorist exploitation, through social media or otherwise, they must immediately contact the Headteacher/DSL and follow the school's normal safeguarding procedures, including discussing the matter with the Deputy CEO and, where deemed necessary, with children's social care at the Local Authority and the local police.

11 Breaches of Policy and Other Issues

11.1 Any breach of this policy and the duties, responsibilities, professional standards and legal obligations referred to will be regarded as a serious matter and action, including disciplinary action in appropriate circumstances, will be taken by the Headteacher (or the Trust Board). In serious cases involving employees, this may lead to dismissal without notice on the grounds of gross misconduct.

11.2 Adults must be aware that any breach of this policy involving a breach of the laws, professional codes or other statutory provisions referred to in this policy may result in legal or other action being taken against them by a body or person other than the school.

Appendix 1: Social Media Request Form

Please complete the form below and return it to your Headteacher

School	
Name of person making the request	
Social media platform	
Date of request	

Who will have access to the account?

What will the account be used for?

What name are you proposing for the social media account?

What will the password and user name be for the account?

Do you agree to follow the trust social media guidelines when using the account?

To be completed by the Headteacher

Approval of the account Y/N _____

Signed

Dated

To be completed by the trust leadership team

Approval of the account Y/N _____

Guidelines shared and signed _____

Social Media and Acceptable use Policy Updated Y/N _____

Signed _____

Dated _____

Appendix 2: Trust Social Media Account Guidelines

All staff using any authorised social media accounts in the school/trust name must agree to follow the guidelines below. Breaches of these guidelines could result in the application of the disciplinary and dismissal policy.

- I understand I have chosen to manage a School/trust social media account and any commitment will not be counted within my directed time
- If I no longer wish to manage the social media account, I will notify my line manager/Headteacher at the earliest opportunity
- I will seek approval from the Headteacher and trust the central leadership team before any trust/School social media accounts are set up
- I will ensure the name of the account has been approved and will not be changed without seeking approval from the Headteacher/trust central leadership team
- I agree I will use the trust/School logo for the profile picture, and I will seek approval before using any other images
- I will share the password and usernames with the Headteacher/trust leadership team and will not change them without approval/notification
- I will not post anything of a personal nature on the account, including personal views or opinions
- I will ensure the account is only used to promote the trust/School and understand I am responsible for making sure all posts are:
    - professional
    - reflective of the trust and Schools image
    - in line with GDPR guidelines
    - subject to the appropriate consent
    - Celebratory
- I will check all posts for spelling and grammar and the appropriateness of images before posting them
- I will not share the username or passwords with anyone else other than the Headteacher unless approval has been sought
- I understand the trust has a right to ask you to remove a post if they feel it does not appropriately reflect the trust/School image
- I understand the trust have the right to terminate the social media account if I fail to comply with any of the statements above

I fully understand the guidelines above and agree to follow them. I understand failure to follow the guidelines could result in the application of the disciplinary and dismissals policy. I can confirm I have read and understood the full social media policy.

Name _____

Signature _____

Date _____

Appendix 3: Personal Social Media Advice for School Staff

Do not accept friend/follow requests from pupils

10 rules for school staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards, use a nickname, or use a contraction
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional and not controversial
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, the school/trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school/trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information
10. Consider uninstalling social media apps from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, remind them of your school's social media policy (if you have one), or tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion, in accordance with your school's social media policy, whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the trust
  - Pupils may then have indirect access through their parents' account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so. The school leadership team can help with this.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request that they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Check your Facebook privacy settings

- Change the visibility of your posts and stories to 'Friends', rather than 'Public'. Otherwise, pupils and their families may be able to see your posts and pictures you've been tagged in, even if you haven't accepted a friend request or they're not on Facebook
- Don't forget to check your old posts and photos – see Facebook's privacy support page for step-by-step instructions on how to do this
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Prevent search engines from indexing your profile so people can't search for you by name – see Facebook's step-by-step instructions
- Remember, some information is always public: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender
- Google your name to see what information about you is visible to the public

Check your Instagram privacy settings

- Change your profile visibility from the default 'Public' setting to 'Private'. Otherwise pupils and their families will be able to see your posts, reels, locations, and who you are following and are followed by. Go to the Instagram Help Centre for support with your privacy settings
- If a pupil or parent followed you before you changed your privacy settings, block them to prevent them seeing your posts
- Be careful about giving third-party apps or websites access to your Instagram account, and check app privileges in your phone to see if any apps currently have access. Sharing your information can put your account at risk and make you visible on search engines, even if you have set your account to 'Private'.
- Remember, some information is always public; your username, your bio and your profile picture
- Google your name to see what information about you is visible to the public

Check your Twitter privacy settings

- If you have a Twitter account specifically for or about teaching, make sure you don't include identifying information about yourself or your school. Use a nickname, for example, 'Miss M'

- Change the visibility on your birth date to ‘You follow each other’ to prevent pupils and parents from seeing this personal information. See Twitter’s profile visibility guidance for more support
- Remember, your username, biography, location, website and profile picture are always public and can be seen by pupils and parents, even if they don’t follow you and you have protected your tweets
- Protect your tweets by checking the box in the ’Audience and tagging’ section of your privacy settings. This will mean only your approved followers can see your tweets
- Google your name to see what information about you is visible to the public