Kirtlington
C.E. School

Social Media Policy

Reviewed and approved by: FGB

Policy Reviewed: October 2026

Future Review: October 2027

Introduction

1. The widespread availability and use of social networking applications bring opportunities to communicate with a wide variety of groups. Whilst recognising the benefits which using social media brings, this policy sets out the principles designed to ensure that all staff members use social media responsibly so that the confidentially of students, staff and the reputation of the school are safeguarded. Staff members must be conscious at all times of the need to keep their personal and professional lives separate when using social media.

2. This policy covers personal use of social media as well as the use of social media for official school purposes. The policy applies to personal media platforms such as networking sites e.g. Facebook, WhatsApp, Instagram; blogs; microblogs such as X; chatrooms; forums; podcasts; open access, online encyclopaedias such as Wikipedia and content sharing sites such as YouTube. However, this list is not exhaustive and new on-line platforms are to be considered automatically covered.

3. This policy also applies to online message boards/forums and comments under news items and other articles.

4. The internet is fast-moving technology and it is impossible to cover all circumstances or emerging media therefore the principles set out in this policy must be followed closely, irrespective of the medium or platform. When using social media, staff should be aware of the potential impact on themselves and the employer.

Purpose of policy and guidance

5. To minimise the reputational, legal and governance risks to the school and its employees, arising from use of social media by staff in both personal and professional capacities.

6. To enable the safe use of social media for the purposes of communication and engagement.

7. To ensure a consistent approach is applied across the school.

8. To identify responsibilities of the school and employees in line with the following policies:

   - Child Protection and Safeguarding
   - Communication policy
   - Data Protection
   - Dignity at Work
   - Professional Standards

- Staff Code of Conduct

Legal implications

9. Staff should be aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of:

- Defamation
- Copyright
- Discrimination
- Contract
- Human Rights
- Protection from harassment
- Criminal Justice
- Data Protection

10. Acceptable use of social networking must comply with UK law. In applying this policy, the school/trust will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

11. For purposes of this policy the term 'public' is used to refer to those outside of the immediate school community (employees, contractors and pupils) and includes (but not exclusively) parents/carers and ex-pupils.

Policy

12. It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

13. The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media for new opportunities for communication, this policy sets out the principles that school staff, governors and contractors are required to follow when using social media.

14. It is essential that pupils/students, 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 students and staff members and the reputation of the school are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

15. The policy also identifies the need for schools to offer a protection for employees who may be harassed or victimised by other members of the school community due to their professional relationship with the school.

16. It provides information and guidance for both professional and personal use and outlines the risks to users and schools, as well as the potential consequences of misuse of the internet and social media.

17. Where staff have concerns about e-safety, these should be raised with the Headteacher or Line managers as soon possible. Advice can also be sought from professional associations and trade unions.

18. This policy equally applies to all employees including teacher trainees, apprentices and any other individuals who work for or provide services on behalf of the school.

19. Each school should have a designated Safeguarding Lead and a Data Protection Lead.

Users' responsibilities

20. Any misuse of social media must be reported promptly to the school or head teacher, whether carried out by pupils, parents/guardians or staff members.

21. All users must be aware that as soon as a post is made online, it is no longer within the private sphere or in the control of the original poster.

22. If an employee is found to have breached this policy, they may be subject to the school's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist with the prosecution of the offenders.

Principles

23. In all communications from members of staff/employees of the school/Academy Trust, staff should:

    a) be conscious at all times of the need to keep personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work and personal interests.

    b) not engage in activities involving social media which may bring school into disrepute.

    c) not represent their personal views as those of the school on any social medium.

    d) not discuss personal information about students, staff and any other professionals that they interact with as part of their job, on social media.

    e) follow safeguarding principles

    f) be open, honest, ethical and professional;

    g) use jargon-free, plain English in professional communication;

    h) be actioned within an agreed time frame;

    i) use the method of communication that is most effective and appropriate to the context, message and audience;

    j) be cost effective.

Monitoring

24. All school ICT systems may be monitored in accordance with the Acceptable Use Policy, so personal privacy cannot be assumed when using school hardware.

25. Schools can monitor the usage of its own internet and email services without prior notification or authorisation from users (staff, contractors and pupils) when justifiable concerns have been raised re: electronic communication. This will be in line with school investigation procedures.

26. The school respects the privacy of its employees. However, postings made on a personal account may attain a wide readership and will therefore be considered public rather than private. Publicly accessible postings may be investigated if there is a suspected breach of this or related policies.

27. When a public post is reported concerning non-employee members of the school community, this will be investigated and responded to by the school. Further action may be taken to assist with the prosecution of the offenders.

Personal use of Social Media

28. Staff members are strongly encouraged not to identify themselves as staff members of their school in their personal social media platforms. This is to prevent information on these sites from being linked with Kirtlington and to safeguard the privacy of staff members. This does not include professional networking sites.

29. Staff should not have contact through any social medium with any student from Kirtlington or any other school. Staff are advised not to communicate on social media platforms with ex-students except via professional networking sites for professional reasons.

30. Staff should decline 'friend requests' from students they receive in their personal social media accounts.

31. Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties must not be discussed on their personal social media platforms.

32. Photographs, videos or any of images of pupils or students should not be published on personal social media platforms without prior permission of parents/carers and the school. Permission should be gained through existing school procedures.

33. School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media unless pre-approved by school leadership.

34. 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.

35. Staff are strongly advised to ensure that they set up and regularly review 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 what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

36. Staff should also select carefully their social media profile picture as it is an extension to their professional image online.

37. Social media should not be used for work related communication. Communication should be through school email or contact details held by the school.

38. Any misuse or abuse of social media must be reported to the Head Teacher as soon as noticed, especially when concerning a pupil, parent/guardian or employee.

Where a member of staff is a parent/guardian as well as an employee of the school/Academy Trust

39. In cases where staff are also parents connected to the school, they are advised to use professional judgment (in reference to child protection and safeguarding policies) when communicating with children or young people also connected to the school community.

40. Staff should only accept friend requests/communicate (when there is a genuine need) with others linked to the school community.

41. This relationship should stand up to scrutiny from a professional perspective and should be appropriate. If a concern of safeguarding arises, this should be reported to the designated safeguarding lead in accordance with school policy.

Risks

42. The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- access to inappropriate material;
- civil or criminal action relating to breaches of legislation;
- cyber bullying by pupils/students;
- damage to the reputation of the school;
- disclosure of confidential information;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;

- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.
- damage to professional reputations with current and future employers.
- virus or other malware (malicious software) infection from infected sites.

External communication with pupils/students

43. Communication with pupils/students will take place face-to-face or through parents via a school email address only

44. A staff member will not communicate with a pupil/student via their personal mobile phone or using personal email addresses. All communication will be through parents via school email.

External communication with parents/carers

45. The school has many lines of communication to maintain positive working relationships with parents/carers. These may include: letters, telephone calls, emails, face-to-face meetings, the website, Facebook, newsletters, progress reports and parents' evenings. Effective communications not only deliver the specific information required, but also enable schools to demonstrate values and ethos. Communication with parents/carers should always reinforce parental support and engagement.

46. Communications will seek to establish open and positive relationships with parents, whilst always ensuring that these relationships are professional. To this end parents should always be addressed in an appropriate manner using formal mediums of communication i.e. telephone, email, letter.

47. Staff will not communicate about school matters with parents/carers or students via any form of networking site, personal mobile or email. Where there is a need to communicate directly with parents/carers (i.e. on school trips) staff will do so through the school office where possible, or through direct calls with number withheld from a personal mobile if essential.

48. School may use Facebook or Instagram posts but this is carefully regulated and not "owned" by individual members of staff. They will only be used by designated members of staff.

Using social media on behalf of Kirtlington School

49. Authorised staff should only use official social media school sites for communicating with parents, the wider community or for professional school marketing and recruitment.

50. Staff should not use personal social media accounts for official school business. Staff must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

51. On school trips staff MUST use official contact details, staff should never give out their personal number to parents, carers or pupils.

52. Personal devices should not be used to access school emails or servers unless with prior agreement.

53. School based staff will be made aware of the implications of using personal devices and will be advised that accessing school communications on personal devices is not an expectation or a condition of employment at the school.

School/Academy Trust websites

54. The school administrator will be responsible for maintaining the content of school websites in line with school Communication Policy. There will be regular communication between the administrator and members of the school leadership to identify what content is appropriate for posting on the school website.

Use of Images

55. Permissions must be sought for images of children/young people to be used in school produced materials, clear reference to online usage needs to be made when permissions are requested.

56. Staff must give permission for their images to be used in relation school produced materials accessible by members of the public (online or in print), whether controlled by the school or not.

    Photographs must be checked carefully to ensure that children who are on the restricted lists are never shown on the website or on social media.

Cyber bullying and Harassment

57. Cyberbullying is making use of information and communications technology, particularly mobile phones and the internet, to deliberately undermine, humiliate or otherwise cause distress to the person on the receiving end. Staff must not use social media and the internet to attack, insult, abuse or defame students, their family members, colleagues, other professionals, or other organisations (including Kirtlington School).

58. Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

59. It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

60. Staff should not personally engage with cyberbullying incidents and should immediately report incidents to the Head Teacher.

61. If a member of Staff is the victim (receives any threats, abuse or harassment from members of the public through their use of social media), they should keep any records of the abuse and if appropriate, screen prints of messages or webpages with time, date and address of the site. Staff must report such incidents using the school's procedures. Support is also available through confidential counselling support.

62. The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work.

63. Staff members and pupils need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, other pupils or parents, can find its way into the public domain even when not intended.

64. If a member of staff is the perpetrator of the incident/s the situation will then be investigated and if appropriate, the Disciplinary or Capability Procedure will be followed.

65. If a pupil is the perpetrator of the incident/s the situation will be initially investigated in line with the school behaviour policy. Where appropriate the police will be consulted.

66. Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police enquires. Staff who are victims of cyber-bullying or harassment will be offered support by their line manager and where suitable, occupational health.

Senior Leadership responsibility in relation to Online Bullying and Harassment

67. The school owes a duty of care to employees to take reasonable steps to provide a safe working environment free from bullying and harassment.

68. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, X, or by any other means.

69. If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

70. Senior Leaders should encourage staff to preserve all evidence by not deleting emails. In addition, logging phone calls and taking screenshots of websites or social media sites would all help towards supporting an investigation. If the incident involves illegal content or

contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police.

71. **In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else**. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.