SOCIAL MEDIA POLICY

June 2025

Signed: ..... Chair Of Governors

..... Headteacher

Next review: June 2028

Building Firm Foundations For Life

Social Media Policy for Schools

Introduction

1. The widespread availability and use of social networking applications bring opportunities to communicate with various groups in new ways. 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 is 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, Googlechat), blogs, microblogs such as X, chatrooms, forums, podcasts, open access, online encyclopaedias, such as Wikipedia, and content sharing sites such as flickr and 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.

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:

- Child Protection and Safeguarding
- Data Protection
- Dignity at Work
- Professional Standards (Staff Code of Conduct)
- Mobile Phone Policy

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. 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

11. 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.

12. 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.

13. 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.

14. The policy also identifies the need for the school 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.

15. 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.

16. Where staff have concerns about e-safety, these should be raised with the Headteacher. Advice can also be sought from relevant professional associations and trade unions.

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

18. Our Designated Safeguarding Lead is the Headteacher, Mr Iain Horner. Our Data Protection Officer is Phil Wicker and he can be contact on 07527363482 (Koala IT). Our Chair of Governors is Craig Morley and he can be contacted via email at cmorley@chesterton.oxon.sch.uk

Users’ responsibilities

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

20. 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.

21. 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 required to assist with the prosecution of the offenders.

Principles

22. In all communications from members of staff/employees of the school, 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) not post on social media regarding the school, its pupils, staff or parents in any way that could be seen as negative, particularly if liable to identify individuals;

f) follow safeguarding principles;

g) be open, honest, ethical and professional;

Monitoring

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

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

25. 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 will be investigated if there is a suspected breach of this or related policies.

26. 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

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

28. Staff should not have contact through any social medium with any student from the named School 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.

29. Staff should decline ‘friend requests’ from students they receive in their personal social media accounts and inform a member of the Senior Leadership Team if they feel uncomfortable about any contact from students past or present.

30. 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.

31. Photographs, videos or any images of pupils or students should not be published on personal social media platforms. They should not be posted on external organisations’ (such as charities linked to the school) social media platforms without prior permission of parents/carers and the school.

32. School email addresses and other official contact details must not be used for setting up personal social media accounts.

33. 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.

34. 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.

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

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

37. Any misuse or abuse of social media must be reported to the Headteacher 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

38. 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.

39. Staff should only accept friend requests/communicate with others linked to the school community when there is a genuine need. Caution should be exercised with maintaining pre-existing links with other members of the school community.

40. 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

41. 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

42. Communication with pupils/students will take place face-to-face or via a staff member's school email address only

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

External communication with parents/carers

44. 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, 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.

45. 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).

46. Staff will not communicate with parents/carers or students via any form of networking site, personal mobile or email. Please see Mobile Phone Policy

47. The school may use Facebook to school event but this will be carefully regulated and not "owned" by individual members of staff. The appropriate permissions will be sought if required. Designated staff will be responsible for the use of this platform.

Using social media on behalf of the named school

48. 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.

49. 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.

50. Schools to provide access to suitable hardware and software where required.

School websites

51. Our website provider will be responsible for maintaining the content of the school website. There will be regular communication between the provider administrator and members of the school leadership to identify what content is appropriate for posting on the school website. The password for the school website will be changed monthly.

Use of Images

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

53. Staff must give permission for their images to be used in relation to school-produced materials that are 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 list are never shown on the websites.

We allow parents to photograph or video school events such as shows or sports day using their mobile phones – but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own.

Cyber bullying and Harassment

54. 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 professionally connected organisations.

55. 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.

56. 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.

57. Staff should not personally engage with cyberbullying incidents and should immediately report incidents to the Headteacher.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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 enquiries. 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

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

65. 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, Twitter, or by any other means.

66. 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.

67. Senior Leaders should encourage staff to preserve all evidence by not deleting emails. In addition, logging phone calls and taking screen-prints of websites 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.

68. 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.