

BOLD FUTURES



Bold Futures Federation Social Media Policy

Document Name: Social Media Policy

Document ID: N/A

Current Version: 3.0

Status: Approved

Signed *L.Coombs, L.manser*
Print Name: L.Coombs, L.Manser

Signed: Robyn Jarret (Governor Approval)
Print Name: Robyn Jarret

BOLD FUTURES



POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
1.0			SM/HB	LT	
1.1	November 2016	Approved	LC	LT	Updated in line with Hampshire guidance
1.2	May 2019	Approved	LC	SK	Updated in line with Hampshire guidance
1.3	September 2023	Approved	AW	RJ	Updated in line with Hampshire guidance
1.4	September 2024	Approved	LC	RJ	Unchanged in line with Hampshire policy
2.0	September 2025		LC		Updated to Bold Futures and detail regarding no phones
3.0	September 2026		LC & LM		Policy comprehensively reviewed and updated to align with Federation safeguarding, online safety, data protection and acceptable-use arrangements.

1. Purpose

Bold Futures Federation recognises that social media is an important part of modern communication and can provide valuable opportunities to communicate with families, celebrate school life, share information and engage with the wider community.

The Federation also recognises that inappropriate use of social media can create significant risks relating to safeguarding, professional boundaries, confidentiality, data protection, cyber security and the reputation of individuals and the Federation.

This policy establishes clear expectations for the safe, responsible and professional use of social media.

It aims to:

- safeguard pupils and members of the Federation community;
 - maintain appropriate professional boundaries between adults and pupils;
 - protect confidential and personal information;
 - ensure official Federation social-media accounts are appropriately managed;
 - establish expectations for personal social-media use where this may affect an individual's professional role;
 - protect staff from inappropriate online contact, bullying or harassment;
 - support compliance with data-protection and safeguarding requirements;
 - ensure concerns arising through social media are reported appropriately; and
 - ensure the Federation communicates online in a professional, respectful and responsible manner.
-

2. Scope

This policy applies across all schools within Bold Futures Federation.

It applies to:

- teaching and support staff;
- senior leaders;
- governors;
- volunteers;
- trainees;
- supply and agency staff;
- contractors;
- consultants; and
- other adults working for or on behalf of the Federation.

Throughout this policy these individuals are referred to collectively as **users** unless a particular provision applies specifically to one group.

The policy applies to both:

- **official use** of social media on behalf of the Federation or one of its schools; and
 - **personal use** where that activity has the potential to affect safeguarding, confidentiality, professional boundaries, colleagues, pupils, families or the reputation of the Federation.
-

3. Definition of Social Media

For the purposes of this policy, social media includes any online platform, application or service that enables users to create, publish, communicate, interact with or share content with others.

This includes, but is not limited to:

- social-networking platforms;
- video and image-sharing platforms;
- messaging services;
- professional networking platforms;
- blogs and microblogs;
- forums and online communities;
- livestreaming platforms;
- group-chat services;
- collaborative online spaces; and
- emerging or future services offering similar functionality.

The principles within this policy apply regardless of the particular platform being used.

4. Relationship with Other Federation Policies

This policy forms part of the Federation's wider framework for safeguarding, professional conduct, online safety and data protection.

It should be read alongside the:

- **Child Protection and Safeguarding Policy;**
- **Online Safety Policy;**
- **Acceptable Use of IT and Digital Technology Policy – Staff, Governors and Other Adults;**
- **Data Protection Policy;**
- **Computing Policy;**
- **Remote Education Policy;**

- **Staff Code of Conduct;**
- **Behaviour Policy;**
- **Anti-Bullying Policy;**
- **Whistleblowing Policy;**

Where social-media activity raises a concern about the safety or welfare of a child, the Child Protection and Safeguarding Policy takes precedence and safeguarding procedures must be followed immediately.

Where an incident involves the inappropriate disclosure, loss or processing of personal data, the Data Protection Policy and Federation data-breach procedures must be followed.

The Acceptable Use of IT and Digital Technology Policy applies where social media is accessed using Federation systems, accounts, devices or networks.

The Online Safety Policy sets out the Federation's wider arrangements for protecting pupils from online harm.

5. General Principles

Users are expected to maintain the same standards of professionalism online as they would in other aspects of their professional role.

Users must:

- maintain appropriate professional boundaries;
- protect the safety and welfare of pupils;
- protect confidential and personal information;
- communicate respectfully and professionally;
- comply with safeguarding and data-protection requirements;
- consider the potential audience and permanence of information posted online;
- recognise that content may be copied, shared, screenshotted or redistributed beyond its intended audience;
- avoid online behaviour that could undermine professional relationships or their role within the Federation; and
- report safeguarding or professional-conduct concerns appropriately.

Privacy settings can reduce access to personal content but cannot guarantee that information will remain private.

Users should therefore consider the possibility that anything posted online could ultimately be seen by pupils, parents, colleagues, senior leaders or members of the public.

6. Official Federation Social-Media Accounts

Official social-media accounts may be used to:

- communicate information to parents and the wider community;
- celebrate pupils' learning and achievements;
- promote events and activities;
- share important announcements;
- celebrate the work of staff and pupils;
- promote Federation values;
- strengthen community engagement; and
- signpost families to useful information or support.

Official accounts must be approved by the Headteacher/Executive Headteacher or another appropriately authorised senior leader.

Only authorised individuals may create, administer or publish content through an official Federation social-media account.

7. Management and Security of Official Accounts

Official social-media accounts are Federation accounts and must not be dependent upon the personal account or personal email address of an individual member of staff wherever the platform permits an organisational arrangement.

Accounts must:

- use an authorised Federation email address wherever possible;
- use secure passwords in accordance with the Acceptable Use of IT and Digital Technology Policy;
- use multi-factor authentication where available and required;
- have appropriate account-recovery arrangements;
- have access restricted to authorised users;
- be reviewed when staff responsibilities change; and
- have access removed promptly when an authorised user leaves the Federation or no longer requires access.

Account passwords must not be publicly displayed or unnecessarily shared.

Where more than one person requires access, this should be managed using the platform's appropriate administrative or delegated-access functions wherever possible rather than sharing individual login credentials.

A senior leader should know which official accounts exist, their purpose and who is authorised to administer them.

8. Publishing Through Official Accounts

Content published on behalf of the Federation must be:

- accurate;
- appropriate;
- professional;
- respectful;
- consistent with Federation values;
- appropriate for the intended audience;
- compliant with safeguarding requirements;
- compliant with the Data Protection Policy; and
- lawful.

Users publishing through official accounts must take reasonable steps to check content before it is published.

Official accounts must not be used:

- for personal purposes;
- to promote an individual's private business or financial interests;
- for party-political campaigning;
- to publish confidential information;
- to criticise individual pupils, parents, colleagues or other members of the community;
- to engage in personal arguments; or
- to publish content that is discriminatory, abusive, threatening or otherwise inappropriate.

Where an error is made, appropriate advice should be sought and the content corrected or removed as necessary.

9. Pupils' Personal Information

Particular care must be taken when publishing information about children.

Staff must not publish:

- pupils' personal contact details;
- home addresses;
- personal email addresses;

- telephone numbers;
- safeguarding information;
- medical information;
- SEND information;
- attendance information;
- confidential educational information; or
- any other information that would unnecessarily compromise a child's privacy or safety.

The Federation will avoid unnecessarily publishing information that could enable a child to be located or contacted.

Where pupil names are used alongside images or information, this must be consistent with the Federation's agreed procedures for safeguarding, data protection and publication.

10. Photographs and Videos of Pupils

Photographs and videos of pupils may only be published through official Federation channels where this is consistent with the Federation's Data Protection Policy, privacy information, safeguarding arrangements and current permissions or preferences held by the school.

Before publishing an image or video, staff must consider whether:

- there is an appropriate purpose for publication;
- the image is suitable and respectful;
- publication could create a safeguarding risk;
- any child shown should not be included because of parental preferences or safeguarding circumstances;
- information visible in the background could identify a pupil's location or disclose confidential information; and
- the accompanying text reveals unnecessary personal information.

Staff must use Federation-approved devices and systems when taking, storing and publishing images of pupils in accordance with Federation procedures.

Images of pupils must not be transferred to or published through a member of staff's personal social-media account.

Detailed arrangements concerning images and recordings are contained within the Data Protection Policy, Online Safety Policy and relevant Federation photography and image-sharing guidance.

11. Personal Social-Media Accounts

The Federation recognises that staff and governors are entitled to use social media in their personal lives.

The Federation does not seek to regulate lawful private activity that has no connection with an individual's professional responsibilities.

However, professional responsibilities and safeguarding obligations continue to apply where personal online activity affects the Federation, pupils, colleagues or the wider school community.

Users should:

- review privacy and security settings regularly;
- consider carefully what personal information they make publicly available;
- consider whether content could reasonably undermine their professional role;
- be aware that other users may copy, screenshot or redistribute content;
- maintain appropriate boundaries with members of the school community; and
- avoid presenting personal views as the views of the Federation.

Users must not use the Federation's name, logo or branding in a way that suggests a personal account is an official Federation account.

12. Professional Boundaries with Pupils

Staff and other adults working with pupils must maintain clear professional boundaries online.

Users must not:

- add, follow or accept current pupils or former pupils under the age of 18 as personal social-media contacts;
- send or accept personal friend/follow requests from current pupils or former pupils under the age of 18;
- communicate privately with current pupils or former pupils under the age of 18 through personal social-media or messaging accounts;
- invite current pupils or former pupils under the age of 18 to join personal groups, channels or online communities;
- share personal contact information with current pupils or former pupils under the age of 18 for the purpose of online communication; or
- use disappearing-message or private-messaging services to communicate with current pupils or former pupils under the age of 18 outside authorised Federation systems.

If a current pupils or former pupils under the age of 18 attempts to contact a member of staff through a personal social-media account, the member of staff should not engage in ongoing communication and should report the contact where appropriate to a senior leader.

Any communication that raises a safeguarding concern must be reported immediately to the DSL.

13. Former Pupils

Professional boundaries can remain relevant after a pupil has left the Federation.

Staff should exercise particular caution regarding personal social-media contact with former pupils, and not engage in contact where the young person remains under the age of 18.

Staff must not use the fact that a pupil has left the school as a means of circumventing professional safeguarding boundaries.

Where there is any uncertainty about whether contact would be appropriate, staff should seek advice from a senior leader before engaging.

Existing family relationships or genuine pre-existing personal relationships may create different circumstances; these should be managed transparently and in accordance with the Staff Code of Conduct and safeguarding expectations.

14. Contact with Parents and Carers

Staff should maintain appropriate professional boundaries with parents and carers online.

School business must be conducted using Federation-approved communication channels, not personal social-media or messaging accounts.

Staff should not normally add or accept parents or carers as new personal social-media contacts where doing so could blur professional boundaries.

The Federation recognises that in local communities staff may already have genuine friendships, family relationships or other pre-existing relationships with parents and carers. The existence of such a relationship is not, by itself, a breach of this policy.

However, staff must ensure that:

- confidential school matters are never discussed through personal social media;

- professional information obtained through their role is not disclosed;
- the relationship does not affect professional judgement;
- safeguarding information is protected; and
- personal communication does not become a substitute for official school communication.

Where a staff member is unsure whether an online relationship creates a professional-boundary concern, they should seek advice from a senior leader.

15. Personal Views and the Federation

Users may express personal views online in their private capacity.

However, they must not:

- claim or imply that personal opinions represent the views of Bold Futures Federation;
- use an official Federation account to express personal views;
- disclose confidential information when discussing educational or professional matters;
- make comments about individual pupils or confidential cases; or
- use their connection with the Federation in a way that could reasonably undermine safeguarding or professional responsibilities.

Where an individual's employment or connection with the Federation is publicly identifiable, they should take particular care to distinguish personal views from official Federation communication.

16. Comments About the Federation, Colleagues, Pupils and Families

Social media must not be used to bully, harass, intimidate or discriminate against another person.

Users must not publish content about colleagues, pupils, parents, governors or other members of the Federation community that:

- breaches confidentiality;
- constitutes bullying or harassment;
- is threatening or abusive;
- is discriminatory;
- discloses personal information without authority;
- creates a safeguarding concern; or

- otherwise breaches professional standards.

Users should use appropriate internal procedures to raise professional concerns about Federation decisions, colleagues or working practices.

Nothing in this policy prevents staff from:

- raising legitimate concerns through the Federation's grievance procedures;
- making a protected disclosure under the Whistleblowing Policy;
- seeking advice from a trade union or professional association; or
- exercising other legal employment rights.

17. Complaints and Critical Comments from Parents or Members of the Public

The Federation recognises that parents and members of the public may sometimes use social media to express concerns or criticism.

Staff should not enter into personal arguments or extended exchanges through personal accounts.

Where criticism relates to the Federation:

- staff should not respond from personal accounts on behalf of the school;
- significant concerns should be brought to the attention of a senior leader;
- responses from official accounts should only be made by an authorised person;
- where appropriate, the individual should be directed towards the Federation's formal complaints procedure; and
- abusive, threatening or safeguarding-related content should be escalated appropriately.

Reasonable criticism should not automatically be treated as harassment.

Where posts become threatening, discriminatory, persistently abusive, defamatory or otherwise potentially unlawful, the Federation may seek appropriate advice and take proportionate action.

18. Online Harassment or Abuse Directed at Staff

The Federation recognises its responsibility to support staff who experience inappropriate online behaviour connected with their work.

This may include:

- threats;
- harassment;
- discriminatory abuse;
- impersonation;
- malicious allegations;
- persistent unwanted contact;
- publication of personal information;
- manipulated or AI-generated content targeting a staff member; or
- coordinated online abuse.

Staff experiencing such behaviour should report it to an appropriate senior leader.

The Federation will consider appropriate support and action depending on the circumstances.

This may include:

- preserving appropriate evidence;
- reporting content to the platform;
- supporting the member of staff to use privacy or blocking tools;
- communicating with parents or other individuals where appropriate;
- seeking HR or legal advice;
- following safeguarding procedures; and
- involving the police where threats, harassment or potentially criminal behaviour are involved.

Staff should not be expected to manage serious work-related online abuse alone.

19. Safeguarding Concerns Identified Through Social Media

Any safeguarding concern discovered through social media must be treated in the same way as a safeguarding concern arising through any other route.

Examples include:

- a pupil disclosing abuse;
- concerning images or videos;
- threats of self-harm or suicide;
- sexualised communication;
- grooming;
- exploitation;
- radicalisation;
- child-on-child abuse;

- threats or coercion; or
- information suggesting that a child may be at risk.

Staff must:

1. report the concern immediately to the DSL or deputy DSL;
2. follow the Child Protection and Safeguarding Policy;
3. preserve relevant information where appropriate;
4. avoid unnecessarily sharing the content;
5. not conduct their own investigation; and
6. follow DSL advice regarding further action.

Staff must not deliberately download, copy or distribute illegal imagery in an attempt to preserve evidence.

Where there is uncertainty, the DSL should seek appropriate specialist advice.

20. Confidentiality and Data Protection

Users must protect personal and confidential information when using social media.

Information obtained through a professional role must not be disclosed through personal social media.

This includes information relating to:

- pupils;
- parents and carers;
- staff;
- safeguarding;
- SEND;
- health;
- attendance;
- behaviour;
- personnel matters;
- complaints;
- Federation business;
- commercially sensitive matters; and
- any other information received in confidence.

Official publication of personal information must comply with the Federation's Data Protection Policy.

Any suspected unauthorised disclosure of personal data must be reported immediately in accordance with the Federation's data-breach procedure.

21. Direct and Private Messaging

Direct or private messaging functions attached to official social-media accounts should only be used where their use has been authorised.

Where an official account receives a private message:

- it should be handled professionally;
- confidential information should not be requested unnecessarily;
- safeguarding disclosures must be passed immediately to the DSL;
- complaints should be directed through appropriate Federation procedures where necessary; and
- the conversation should be moved to an appropriate official communication channel where continued discussion is required.

Official social-media messaging must not become an informal substitute for safeguarding, complaints or other established Federation systems.

22. Social Media and Artificial Intelligence

The increasing use of artificial intelligence creates additional considerations for social media.

Users must not use AI to create or manipulate content for official Federation social-media accounts in a way that:

- misrepresents pupils, staff or events;
- creates false or misleading information;
- compromises safeguarding;
- breaches confidentiality or data protection;
- infringes copyright or intellectual-property rights; or
- could reasonably deceive the intended audience about a significant matter.

Personally identifiable, confidential or safeguarding information must not be entered into an unauthorised AI system to create social-media content.

Where AI-generated or AI-assisted content is used officially, the person publishing it remains responsible for checking its accuracy, appropriateness and compliance with Federation policy.

Concerns involving deepfakes, AI-generated images, impersonation or other synthetic media involving pupils or staff should be reported through the appropriate safeguarding or professional-conduct procedure.

23. Copyright and Intellectual Property

Content published through Federation social media must respect copyright and intellectual-property rights.

Staff should:

- use content created by the Federation or appropriately licensed for use;
- obtain appropriate permission where required;
- provide attribution where necessary; and
- avoid copying images, music, video or other protected content simply because it is publicly available online.

The use of AI does not remove the need to consider copyright and intellectual-property requirements.

24. Monitoring of Official Accounts

Official Federation social-media accounts will be monitored appropriately.

The Federation may:

- review content published through its accounts;
- moderate or remove inappropriate comments where platform functionality permits;
- restrict or block users where necessary to protect pupils, staff or the school community;
- retain information relating to significant incidents; and
- report unlawful or harmful content to platforms or relevant authorities.

Moderation decisions should be proportionate and should not be used simply to prevent legitimate criticism.

25. Personal Social Media and Monitoring

The Federation does not routinely monitor employees' private social-media accounts. However, online searches are carried out during the recruitment process inline with Safer Recruitment guidelines.

The Federation may need to consider publicly available or appropriately reported social-media content where there is a legitimate concern relating to:

- safeguarding;
- professional conduct;
- bullying or harassment;
- discrimination;
- confidentiality;
- data protection;
- reputational risk connected with professional responsibilities; or
- potential criminal activity.

Any investigation will be undertaken in accordance with appropriate Federation procedures.

26. Governors

Governors are expected to follow the same principles of confidentiality, safeguarding and responsible online conduct as other adults acting on behalf of the Federation.

Governors must:

- maintain the confidentiality of information received through their governance role;
- not use personal social media to disclose or debate confidential governing-body business;
- not present personal opinions as decisions or views of the Governing Body;
- use authorised channels for official Federation communication;
- maintain appropriate boundaries with pupils; and
- refer media or public enquiries concerning Federation matters to the appropriate authorised person.

Where a governor has access to an official social-media account, the same security and publication requirements apply.

27. Breaches of this Policy

Concerns about possible breaches will be considered appropriately and proportionately.

Depending upon the circumstances, action may include:

- advice or guidance;
- additional training;
- removal of permission to administer Federation social-media accounts;
- removal or correction of content;
- action under the Acceptable Use Policy;
- safeguarding action;

- data-protection action;
- disciplinary procedures;
- governor conduct procedures;
- referral to the Local Authority Designated Officer where appropriate;
- referral to external agencies; and/or
- police involvement where criminal activity is suspected.

Where a concern relates to the safety of a child, safeguarding procedures take priority.

28. Reporting Concerns

Safeguarding concern involving a child

Report immediately to the DSL or deputy DSL and follow the Child Protection and Safeguarding Policy.

Personal-data breach

Report immediately in accordance with the Data Protection Policy and Federation data-breach procedure.

Concern about the conduct of a member of staff or volunteer

Follow the Federation's procedures for allegations and low-level concerns.

Concern about the Headteacher

Follow the procedures contained within the Child Protection and Safeguarding Policy, Staff Code of Conduct and/or Whistleblowing Policy as appropriate.

Cyber-security concern

Follow the Acceptable Use of IT and Digital Technology Policy and relevant cyber-security procedures.

Online harassment or abuse directed at a member of staff

Report to the Headteacher or another appropriate senior leader.

29. Training and Awareness

Relevant staff will be made aware of this policy and the Federation's expectations for social-media use.

Training and guidance may include:

- professional boundaries;
- safeguarding;
- privacy settings;
- data protection;
- official-account security;
- publication of pupil images and information;
- online harassment;
- emerging social-media risks;
- artificial intelligence and synthetic media; and
- reporting procedures.

Staff responsible for official Federation social-media accounts should receive appropriate guidance before being given access.

30. Review

This policy will be reviewed at least annually and sooner where necessary because of:

- changes to safeguarding guidance;
 - changes to data-protection requirements;
 - significant changes in social-media technology;
 - emerging technologies, including artificial intelligence;
 - significant incidents;
 - changes to Federation communication arrangements; or
 - learning arising from safeguarding or conduct reviews.
-

Appendix 1 – Social Media: Quick Guide for Staff and Governors

Official accounts

Do:

- use only authorised Federation accounts;
- check content before publishing;
- protect account login details;
- use MFA where required;

- follow pupil image/publication arrangements;
- communicate professionally;
- report safeguarding concerns immediately.

Do not:

- use personal accounts for Federation business;
- publish confidential information;
- publish pupil information without appropriate authority;
- engage in personal arguments;
- share official account credentials unnecessarily;
- post content that could compromise safeguarding.

Personal accounts

Do:

- review your privacy settings;
- maintain professional boundaries;
- assume content could become public;
- think carefully before posting about work-related matters;
- report inappropriate contact from pupils.

Do not:

- communicate privately with current pupils;
- accept current pupils as personal social-media contacts;
- use personal accounts for school business;
- discuss confidential pupils, families or colleagues;
- publish Federation information obtained through your professional role;
- present personal opinions as Federation views.

If something goes wrong

Safeguarding concern → DSL immediately

Data breach → follow Data Protection procedure immediately

Cyber-security concern → follow Acceptable Use/cyber-security procedure

Online abuse or harassment → senior leader

Concern about an adult's conduct → safeguarding/low-level concern/allegations procedure
