



BRIGHTFIELD

ACADEMY

Inclusion. Choice. Growth.



SOCIAL MEDIA & ONLINE COMMUNICATIONS POLICY

Promoting safe, respectful and professional use of digital platforms to protect our learners, staff and the Brightfield Academy community.



SAFE



RESPECTFUL



RESPONSIBLE



PROFESSIONAL



INCLUSIVE



POLICY VERSION
1.0



LAST UPDATED
JUNE 2026



REVIEW DATE
JUNE 2027



Social Media & Online Communications Policy

1. Policy Introduction

Purpose and Aim

Brightfield Academy recognises that social media and online communication are valuable tools for communication, collaboration, learning and promoting the Academy. However, their use also presents safeguarding, professional, reputational and data protection risks that must be managed appropriately.

The purpose of this policy is to:

- promote the safe, responsible and professional use of social media and online communication;
- safeguard children and young people from potential harm arising through online interactions;
- protect the privacy, dignity and confidentiality of learners, families and staff;
- establish clear expectations for the use of personal and organisational social media accounts;
- maintain appropriate professional boundaries between staff, volunteers, learners and their families;
- protect the reputation of Brightfield Academy and those working on its behalf;
- ensure compliance with safeguarding legislation, UK GDPR and other relevant statutory guidance.

This policy supports Brightfield Academy's commitment to providing a safe learning environment where safeguarding remains everyone's responsibility.

Policy Statement

At Brightfield Academy, we recognise that responsible use of social media can enhance communication, celebrate achievement and strengthen relationships with our community.

Equally, inappropriate online activity has the potential to compromise safeguarding, damage professional relationships and undermine confidence in the Academy.

Our values of

Inclusion

Choice

Growth

extend to all online activity undertaken by those representing Brightfield Academy. Everyone working on behalf of the Academy is expected to demonstrate professionalism, respect, integrity and sound judgement whenever using social media or communicating online.

Safeguarding considerations will always take priority over publicity or promotion.

Responsibility and Review

Overall responsibility for this policy rests with the Directors of Brightfield Academy.

Designated Safeguarding Lead (DSL)

Kathleen Larcombe

Telephone: 07545 123930

Email: dsl@brightfieldacademy.co.uk

Deputy Designated Safeguarding Lead (DDSL)

Nik Larcombe

Telephone: 07395 111919

Email: nik@brightfieldacademy.co.uk

Policy Owner

Directors

Brightfield Academy

Date Approved: June 2026

Review Date: June 2027

This policy will be reviewed annually, or sooner where changes in legislation, technology, safeguarding guidance or organisational practice require.

2. Scope of this Policy

This policy applies to all individuals working on behalf of Brightfield Academy, including:

- Directors
- Employees
- Volunteers
- Contractors
- Agency staff
- Placement students
- Visitors acting on behalf of the Academy
- External professionals delivering services for Brightfield Academy

The policy applies to all online communication, including:

- Personal social media accounts
- Official Brightfield Academy accounts
- Messaging applications
- Video conferencing platforms
- Discussion forums
- Blogs
- Live streaming platforms
- Any future online communication platforms

The expectations within this policy apply whether activity takes place:
during working hours;
outside working hours where the individual can be identified with Brightfield Academy;
using Academy equipment;
using personal devices;
on or off Academy premises.

3. Legislative and Statutory Framework

This policy has been developed in accordance with:

Keeping Children Safe in Education (KCSIE)

Working Together to Safeguard Children

Data Protection Act 2018

UK General Data Protection Regulation (UK GDPR)

Human Rights Act 1998

Equality Act 2010

Education Act 2002

Online Safety Act

Guidance for Safer Working Practice for Adults Working with Children and Young People

Buckinghamshire Safeguarding Children Partnership procedures

This policy should be read alongside the following Brightfield Academy policies:

Child Protection & Safeguarding Policy

Staff Code of Conduct

Online Safety Policy

Data Protection Policy

Photography and Video Consent procedures

Managing Allegations and Low-Level Concerns Policy

Acceptable Use of Technology Policy

4. Core Principles

Brightfield Academy believes that social media should be used responsibly, professionally and safely.

All online activity should:

safeguard children and young people;

maintain appropriate professional boundaries;

protect confidential information;

promote respectful communication;

support positive relationships;

uphold the reputation of Brightfield Academy;

comply with safeguarding and data protection legislation.

Every member of staff shares responsibility for ensuring that their online behaviour reflects the Academy's values and professional standards.

Online conduct should always be considered with the understanding that information shared electronically may remain publicly accessible indefinitely, even after deletion.

5. Personal Social Media Accounts

Brightfield Academy recognises that staff, volunteers and other adults working on behalf of the Academy have the right to use personal social media in their own time.

However, individuals should recognise that their online activity may affect their professional reputation, the reputation of Brightfield Academy and the confidence placed in them by learners, parents/carers and colleagues.

Staff should always exercise good judgement and consider whether content shared online could:

- undermine professional relationships;
- compromise safeguarding;
- damage public confidence in the Academy;
- bring Brightfield Academy into disrepute.

Online activity should reflect the same standards of professionalism expected within the workplace.

5.1 Personal Account Expectations

Staff, volunteers and contractors must:

- maintain appropriate professional boundaries at all times;
- regularly review and maintain the privacy settings on personal social media accounts;
- enable two-factor authentication wherever available;
- avoid sharing personal information that could compromise their own safety or that of others;
- consider that anything shared online may become public, even where privacy settings are applied;
- report any safeguarding concerns identified through social media in accordance with the Academy's Safeguarding Policy.

5.2 Contact with Learners and Families

To maintain appropriate professional boundaries, staff and volunteers must **not**:

- send or accept friend requests from current learners;
- follow, subscribe to or connect with learners using personal accounts;
- communicate with learners through personal messaging applications;
- share personal telephone numbers or personal email addresses with learners;
- participate in private online groups involving learners unless these are authorised by the Academy.

Staff should also avoid establishing personal social media relationships with parents, carers or family members where doing so could blur professional boundaries or compromise objectivity.

Where an existing relationship exists prior to employment, staff should declare this to the Head of Provision so that any potential conflicts of interest can be managed appropriately.

5.3 Former Learners

Professional boundaries continue after a learner leaves Brightfield Academy.

Staff should exercise professional judgement before connecting with former learners through personal social media.

No member of staff should establish personal social media contact with any former learner who remains under the age of 18.

Connections with adult former learners should only occur where there is no safeguarding concern, no conflict of interest and no risk to professional boundaries.

6. Professional Boundaries Online

Professional boundaries that apply within the Academy also apply online.

All communication with learners should be:

- professional;
- transparent;
- respectful;
- appropriate to the individual's role.

Staff should use only Academy-approved communication methods when communicating with learners or parents/carers.

Communication should never become overly familiar or personal.

Staff must not:

- engage in inappropriate humour or conversations;
- exchange personal photographs;
- communicate late at night unless required for safeguarding or emergency purposes;
- share information about their private lives that could compromise professional relationships;
- discuss learners, families or colleagues through personal online accounts.

Any attempted inappropriate online contact from a learner or parent/carer should be politely declined, recorded where appropriate and reported to the Designated Safeguarding Lead.

7. Association with Brightfield Academy

Individuals should recognise that they may be associated with Brightfield Academy even when using personal social media accounts.

Where an individual identifies themselves as working or volunteering for Brightfield Academy, or can reasonably be identified as such, their online conduct may affect the reputation of both themselves and the Academy.

Staff must not publish content that:

- could bring Brightfield Academy into disrepute;
- damages public confidence in the Academy;
- criticises or ridicules learners, parents/carers or colleagues;
- contains discriminatory, offensive or abusive language;
- discloses confidential information;
- comments publicly on safeguarding matters, complaints, disciplinary matters or ongoing investigations;
- could reasonably undermine trust in their professional role.

Personal opinions expressed online should not be presented as representing the views of Brightfield Academy.

Where appropriate, staff should make clear that views expressed are their own.

8. Online Reputation

Every member of staff shares responsibility for protecting the reputation of Brightfield Academy.

Before posting online, staff should consider:

- Would I be comfortable if this was seen by learners or parents?
- Could this undermine confidence in my professional role?
- Could this damage the reputation of Brightfield Academy?
- Does this align with the Academy's values of Inclusion, Choice and Growth?

If the answer to any of these questions is uncertain, the content should not be posted. Staff who become aware of online content that may damage the reputation of Brightfield Academy should report this promptly to the Head of Provision or Directors.

9. Official Brightfield Academy Social Media Accounts

Brightfield Academy uses official social media platforms to celebrate achievements, share information, communicate with the wider community and promote the Academy in a positive, safe and professional manner.

Only authorised members of staff may create, administer or publish content on behalf of Brightfield Academy.

Official Academy accounts remain the property of Brightfield Academy at all times.

9.1 Authorised Users

The Directors will determine which staff members are authorised to manage official social media accounts.

Authorised users must:

- understand this policy;
- complete appropriate safeguarding and data protection training;
- maintain professional standards at all times;
- use Academy-approved email addresses where possible;
- ensure account access is appropriately secured.

Where practicable, official accounts should have at least two authorised administrators to ensure continuity and accountability.

Passwords must be kept secure and changed whenever authorised personnel leave the organisation.

9.2 Professional Standards

Content published on official Brightfield Academy accounts must:

- promote the Academy positively;
- reflect the values of Inclusion, Choice and Growth;
- be respectful and inclusive;
- be accurate and appropriate;
- promote safeguarding and wellbeing;
- comply with copyright and data protection legislation.

Posts should be written professionally and avoid language or humour that could reasonably cause offence or misunderstanding.

9.3 Interaction with the Public

When responding to comments or messages, authorised staff should:

- remain courteous and professional;
- avoid becoming involved in arguments or online disputes;
- avoid discussing individual learners or families;
- move sensitive conversations to appropriate offline communication wherever possible;
- report safeguarding concerns immediately to the Designated Safeguarding Lead.

Comments containing abusive, discriminatory, threatening or inappropriate material may be removed where platform settings permit.

Persistent misuse of Academy social media platforms may result in users being blocked or referred to the appropriate authorities where necessary.

10. Confidentiality and Anonymity

Safeguarding and confidentiality remain essential responsibilities both online and offline. Staff must never publish information that could identify or compromise:

- learners;
- former learners;
- parents or carers;
- staff members;
- safeguarding investigations;
- complaints;
- disciplinary matters;
- confidential Academy business.

Particular care should be taken to ensure that photographs, comments or seemingly harmless information cannot unintentionally identify vulnerable learners.

Staff must never discuss safeguarding matters through social media.

10.1 Protecting Learner Identity

Unless explicit written consent has been obtained, staff must not publish:

- full names of learners;
- personal addresses;
- telephone numbers;
- personal email addresses;
- medical information;
- SEND information;
- safeguarding information;
- attendance information;
- behavioural information;
- assessment information.

Where images are published with consent, accompanying text should avoid revealing unnecessary personal information.

11. Photography, Video and Live Streaming

Brightfield Academy recognises that photographs and videos can celebrate achievement and promote learning. However, their use must always prioritise safeguarding, dignity and privacy. Images and recordings must only be used where they are:

- appropriate;
- respectful;
- necessary;
- supported by valid consent.

11.1 Consent

Photographs or videos of learners will only be taken, stored or published where appropriate written consent has been obtained in accordance with the Academy's Photography and Video Consent procedures.

Consent will specify how images may be used, including:

- Academy website;
- official social media;
- newsletters;
- promotional materials;
- displays;
- printed publications.

Consent may be withdrawn at any time.

Where consent is withdrawn, Brightfield Academy will cease using future images wherever reasonably practicable.

11.2 Appropriate Images

Images should:

- present learners positively;
- preserve dignity and respect;
- reflect Academy activities appropriately;
- avoid unnecessary identification of individuals;
- avoid displaying personal information;
- avoid highlighting vulnerabilities.

Staff should carefully consider whether publication could unintentionally reveal:

- learner locations;
- daily routines;
- transport arrangements;
- safeguarding considerations;
- sensitive personal circumstances.

11.3 Storage of Images

Photographs and videos taken for Academy purposes should be stored only on approved Academy systems.

Staff must not routinely use personal mobile phones or personal cloud storage to retain Academy photographs.

Where personal devices are exceptionally authorised, images must be transferred securely to Academy systems and deleted from the personal device as soon as reasonably practicable.

11.4 Live Streaming

Live streaming involving learners presents additional safeguarding considerations.

Live streaming should only take place:

- where educationally or operationally appropriate;
- following approval by the Directors;
- where appropriate consent has been obtained;
- following consideration of safeguarding risks.

Live streams should never reveal confidential information or place learners at unnecessary risk.

12. Reporting Online Safeguarding Concerns

Where staff become aware of concerning online content relating to a learner, they should not engage directly with the learner through social media.

Instead they should:

- preserve evidence where appropriate (for example by taking a screenshot);
- avoid sharing the content with others unless required for safeguarding;
- report concerns immediately to the Designated Safeguarding Lead;
- follow the Academy's Child Protection and Safeguarding Policy.

Examples may include:

- indications of self-harm;
- online exploitation;
- child sexual exploitation;
- child criminal exploitation;
- grooming;
- county lines activity;
- cyberbullying;
- extremist content;
- missing children;
- significant emotional distress.

Where a child is believed to be at immediate risk of harm, emergency safeguarding procedures should be followed without delay.

13. Breaches of this Policy

Failure to comply with this policy may place learners, colleagues or the Academy at risk.

Any breach will be considered on its individual circumstances and may result in:

- informal advice or guidance;
- additional supervision or training;
- management action;
- disciplinary proceedings;
- referral to safeguarding agencies;
- referral to professional bodies where appropriate;
- termination of employment or voluntary placement in cases of serious misconduct.

Where online behaviour indicates that a child may be at risk of harm, safeguarding procedures will always take precedence over disciplinary processes.

Where criminal offences may have been committed, the Academy will work with the Police and other statutory agencies as appropriate.

14. Monitoring and Compliance

Brightfield Academy will monitor the implementation of this policy to ensure that online activity remains safe, professional and consistent with safeguarding responsibilities.

Monitoring may include:

- reviewing official Academy social media accounts;
- auditing consent records for photographs and videos;
- reviewing safeguarding concerns relating to online activity;
- monitoring trends and emerging risks;
- reviewing incidents involving inappropriate online communication;
- evaluating staff understanding through supervision and training.

Monitoring will always be undertaken lawfully, proportionately and in accordance with data protection legislation.

15. Training and Awareness

Brightfield Academy recognises that social media platforms and online risks continue to evolve. All staff, volunteers and contractors will receive appropriate information, instruction and training relating to:

- safe and professional use of social media;
- online safeguarding;
- maintaining professional boundaries;
- confidentiality and information sharing;
- data protection;
- photography and video consent;
- identifying and reporting online safeguarding concerns;
- emerging online risks and technologies.

Training will be provided:

- during induction;
- through safeguarding updates;
- during annual safeguarding training;
- whenever significant changes in legislation or technology occur.

Staff are expected to remain familiar with this policy and seek advice whenever they are uncertain about appropriate online practice.

16. Responsibilities

Every adult working on behalf of Brightfield Academy shares responsibility for maintaining safe and professional online practice.

Directors are responsible for:

- approving this policy;
- ensuring appropriate governance;
- promoting a positive safeguarding culture.

The Designated Safeguarding Lead is responsible for:

- advising staff on safeguarding concerns arising from online activity;
- managing safeguarding referrals relating to social media;
- supporting investigations where necessary;
- ensuring safeguarding records are maintained.

Managers are responsible for:

- promoting compliance with this policy;
- challenging inappropriate practice;
- supporting staff in maintaining professional standards.

Staff and Volunteers are responsible for:

- following this policy at all times;
- maintaining professional boundaries;
- protecting confidential information;
- reporting safeguarding concerns promptly;
- seeking advice whenever unsure.

17. Related Policies

This policy should be read alongside the following Brightfield Academy documents:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Online Safety Policy
- Acceptable Use of Technology Policy
- Data Protection Policy
- Photography and Video Consent Procedures
- Managing Allegations and Low-Level Concerns Policy
- Confidentiality Policy
- Behaviour Policy
- Complaints Policy

18. Policy Review

This policy will be reviewed:

- annually;
- following changes to legislation or statutory guidance;
- following significant safeguarding incidents;
- where lessons learned indicate that amendments are required.

The Directors retain responsibility for ensuring this policy remains effective, proportionate and reflective of current safeguarding best practice.



BRIGHTFIELD
— A C A D E M Y —



BRIGHTFIELD ACADEMY

Inclusion. Choice. Growth.



SOCIAL MEDIA & ONLINE COMMUNICATIONS *Quick Guide* FOR STAFF

✓ DO



Maintain professional boundaries.

Keep all online interactions respectful, appropriate and professional.



Use only approved Brightfield communication systems.

Use official channels for all communication with learners and families.



Report safeguarding concerns immediately.

Speak to the DSL if you see or receive something concerning online.



Review your privacy settings regularly.

Control who can see your information and posts.



Use strong passwords and two-factor authentication.

Protect your accounts and Academy data.



Consider whether your online activity reflects Brightfield's values. *Inclusion. Choice. Growth.*



Obtain written consent before sharing photographs or videos.

Follow our Photo & Video Consent procedures.



Protect confidential information at all times.

Do not share personal or sensitive details online.



Ask for advice if you are unsure.

If in doubt, speak to the DSL or a member of leadership.

✗ DON'T



Accept friend requests from learners.

Do not connect with learners on personal accounts.



Send friend requests to learners.

This can blur professional boundaries.



Use personal messaging apps to communicate with learners.

Use only approved Academy systems.



Share confidential information online.

This includes safeguarding, personal or internal matters.



Post photographs without appropriate consent.

Always obtain written consent first.



Identify vulnerable learners.

Do not share names, locations or details that could identify individuals.



Comment publicly on safeguarding matters.

Report concerns privately to the DSL.



Engage in arguments while representing Brightfield Academy.

Stay professional and respectful.



Assume deleted content has disappeared permanently.

Once online, content can last forever.

Before You Post, Ask Yourself:

- ✓ Is it professional?
- ✓ Is it respectful?
- ✓ Is it safe?
- ✓ Does it protect children?
- ✓ Would I be comfortable if a parent, learner or inspector saw it?



If the answer is NO or I'M NOT SURE,
don't post it.



PHOTO & VIDEO PUBLICATION CHECKLIST

- | | |
|---|--|
| ☒ Appropriate written consent has been obtained. | ☒ Uniforms, badges or documents do not reveal unnecessary information. |
| ☒ Consent covers the intended use. | ☒ No safeguarding concerns apply to the learner(s). |
| ☒ Consent has not been withdrawn. | ☒ The image reflects Brightfield Academy positively. |
| ☒ The image promotes dignity and respect. | ☒ Approval has been obtained where required. |
| ☒ No confidential or personal information is visible. | ☒ Images are stored securely in line with our Data Protection Policy. |



FINAL CHECK:

Would this image still be appropriate if it remained online for the next ten years?

If you have any doubts, do not publish.

Safeguarding is everyone's responsibility. Professional curiosity protects children.



INCLUSION



CHOICE



GROWTH

