

FOOTSTEPS TRUST SOCIAL MEDIA POLICY

1. Policy Statement

Footsteps Trust recognises that social media and digital communication are an important part of modern life and can provide valuable opportunities for learning, communication, creativity and community engagement. However, social media also presents significant safeguarding, wellbeing, privacy and reputational risks.

As an Alternative Provision, the Academy recognises that some students may be particularly vulnerable to:

- Online exploitation.
- Grooming.
- Cyberbullying.
- Child Criminal Exploitation (CCE).
- Child Sexual Exploitation (CSE).
- Radicalisation.
- Misinformation and disinformation.
- Sextortion.
- Harmful online communities.
- Online misogyny and hate-based content.

This policy sets out expectations for safe, respectful and responsible use of social media and other online platforms by students. It should be read alongside the Academy's:

- Safeguarding and Child Protection Policy.
- Online Safety Policy.
- Behaviour Policy.
- Anti-Bullying Policy.
- Data Protection and Privacy Policies.

2. Legislative Framework

This policy has regard to:

- Keeping Children Safe in Education (KCSIE) 2026.
- Working Together to Safeguard Children.
- Children Act 1989 and 2004.
- Online Safety Act 2023.
- Data Protection Act 2018.
- UK GDPR.
- Human Rights Act 1998.

Date of Issue: September 2026

Date of Review: September 2027

- Equality Act 2010.
- Defamation Act 2013.
- Communications Act 2003.
- Malicious Communications Act 1988.
- Counter-Terrorism and Security Act 2015 (Prevent Duty).

The Academy recognises that online safety is an integral part of safeguarding and child protection. Current safeguarding expectations require schools and alternative provisions to address online risks in the same way as offline risks.

3. Aims

The Academy aims to:

- Promote safe, responsible and respectful online behaviour.
- Protect students from online harm.
- Educate students about digital citizenship.
- Support positive mental health and wellbeing.
- Safeguard students from bullying, exploitation and abuse.
- Promote responsible use of social media.
- Protect the reputation of students, staff and the Academy.
- Ensure compliance with safeguarding and legal responsibilities.

4. Definition of Social Media

For the purposes of this policy, social media refers to online platforms, applications and services that allow users to create, share or interact with content and other users.

Examples include:

- TikTok.
- Snapchat.
- Instagram.
- Facebook.
- X (formerly Twitter).
- YouTube.
- WhatsApp.
- Discord.
- Telegram.
- Gaming platforms with communication features.
- Blogs, forums and discussion boards.

This list is not exhaustive.

5. Roles and Responsibilities

Trustees and Senior Leaders

Will:

- Promote a culture of online safety.
- Ensure appropriate safeguarding policies are in place.
- Monitor online safety incidents and trends.
- Ensure staff receive appropriate training.

Designated Safeguarding Lead (DSL)

Will:

- Oversee online safety and digital safeguarding.
- Respond to safeguarding concerns arising online.
- Liaise with external agencies where necessary.
- Provide advice and support to staff, students and families.
- Monitor emerging online risks.

Staff

Will:

- Promote safe online behaviour.
- Reinforce online safety education.
- Report safeguarding concerns promptly.
- Maintain professional boundaries online.
- Follow staff code of conduct expectations.

Parents and Carers

Will:

- Support safe use of technology.
- Monitor online activity where appropriate.
- Work in partnership with the Academy.
- Report concerns affecting their child.

Students

Will:

- Use social media responsibly.
- Treat others with respect online.
- Report concerns immediately.
- Follow Academy expectations.
- Protect themselves and others online.

6. Student Responsibilities

Students should:

- Think carefully before posting content online.
- Understand that online content may remain accessible indefinitely.
- Maintain respectful communication.
- Consider their digital reputation.
- Act responsibly when using technology.
- Follow age restrictions of social media platforms.
- Respect the privacy of others.
- Report concerning content.

Students should recognise that online conduct may affect:

- Personal safety.
- Relationships.
- Educational opportunities.
- Employment opportunities.
- The reputation of themselves and others.

7. Unacceptable Online Behaviour

Students must not use social media or digital platforms to:

- Bully, harass or intimidate others.
- Share hateful, discriminatory or offensive content.
- Threaten others.
- Encourage violence.
- Promote self-harm or suicide.
- Share inappropriate images or videos.
- Share private or confidential information.
- Create fake accounts to impersonate others.
- Record or distribute images without consent.
- Access or share illegal material.
- Promote extremist views.
- Engage in online abuse.

Such behaviour may result in safeguarding intervention, disciplinary action and/or referral to external agencies.

8. Cyberbullying

Cyberbullying is bullying that takes place using technology or online platforms.

Examples include:

- Sending abusive messages.
- Sharing embarrassing content.
- Excluding individuals from online groups.
- Posting harmful comments.
- Creating fake profiles.
- Sharing rumours.

The Academy adopts a zero-tolerance approach to cyberbullying.

Students must:

- Not participate in cyberbullying.
- Save evidence where possible.
- Report incidents to a trusted adult immediately.

9. Online Safeguarding Risks

Students should be aware of risks including:

Grooming

Where an individual attempts to build a relationship with a child for the purpose of abuse or exploitation.

Child Sexual Exploitation (CSE)

Where online contact may be used to manipulate, coerce or exploit children.

Child Criminal Exploitation (CCE)

Where digital communication may facilitate criminal activity or county lines involvement.

Sextortion

A form of online blackmail involving real or manipulated intimate images.

Radicalisation

Exposure to extremist content and harmful ideologies online.

Fraud and Scams

Attempts to obtain money, personal information or access to accounts.

Students should immediately report any concerns to the DSL or safeguarding team.

10. Artificial Intelligence, Deepfakes and Emerging Technologies

The Academy recognises emerging online risks associated with:

- Artificial intelligence.
- Deepfake imagery.
- Synthetic media.
- AI-generated abuse.
- Online impersonation.

Students must not:

- Create fake images of others.
- Share manipulated images.
- Use AI to harass, threaten or embarrass others.

Any use of technology causing harm to others will be treated as a safeguarding and behaviour matter.

11. Privacy and Personal Information

Students should:

- Never share passwords.
- Protect personal information.
- Use privacy settings appropriately.
- Consider who may view online content.
- Be cautious when sharing photographs or videos.

Students should avoid sharing:

- Home addresses.
- Telephone numbers.
- School locations in real time.
- Financial information.
- Personal identification details.

12. Images, Video and Recordings

Students must not:

- Record staff without permission.
- Record other students without permission.
- Share images or videos that may cause harm or embarrassment.
- Post recordings of incidents within the Academy.

Images and recordings may only be made or shared where authorised.

13. Social Media and the Reputation of the Academy

Students should behave online in a way that reflects Academy values.

Content that may damage:

- The reputation of the Academy.
- The reputation of staff.
- The reputation of other students.

may be investigated and addressed through Academy procedures.

Students should remember that online behaviour can have consequences even when activity occurs outside school hours.

14. Reporting Concerns

Students should report:

- Cyberbullying.
- Online harassment.
- Grooming attempts.
- Exploitation concerns.
- Extremist content.
- Sextortion.
- Harmful online challenges.
- Suspicious communication.

Concerns should be reported to:

- The Designated Safeguarding Lead.
- A Deputy DSL.
- Any trusted member of staff.

Urgent concerns will be managed through safeguarding procedures.

15. Academy Response

The Academy may:

- Investigate reports.
- Gather evidence.
- Meet with students and families.
- Implement safeguarding interventions.
- Apply behaviour sanctions.
- Restrict Academy technology access.
- Refer matters to external agencies or Police where appropriate.

Responses will be proportionate, fair and focused on safeguarding.

16. Staff Use of Social Media

Staff must:

- Maintain professional boundaries.
- Not communicate with students through personal social media accounts.
- Follow the Staff Code of Conduct.
- Report concerning online interactions.

Staff should avoid behaviour that could:

- Create conflicts of interest.
- Compromise safeguarding.
- Damage professional reputation.

17. Education and Awareness

Students will receive ongoing education regarding:

- Online safety.
- Digital citizenship.
- Cyberbullying.
- Privacy and security.
- Healthy online relationships.
- Misinformation and disinformation.
- Social media pressures.
- Online consent.
- AI and emerging technologies.

Online safety education will be embedded throughout the curriculum and safeguarding programme.

18. Monitoring and Review

The Academy will monitor:

- Online safety incidents.
- Cyberbullying reports.
- Safeguarding concerns.
- Emerging digital risks.
- Policy effectiveness.



This policy will be reviewed annually or sooner if required by changes in legislation or safeguarding guidance.