

Responsible body	Title of policy	
Governing body	Social Media Policy	

Our Vision



Ratified by the Governing Body: September 2026

Date for review: Annually or earlier following significant legislative, regulatory or organisational change

Signed by:

L. Screen

Chair of governors: Lisa Screen

Tracie Langfield

Headteacher : Tracie Langfield

Author

Updated

Page

Tracie Langfield

September 2026

1 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

1. Statement of Intent

Astley CE Primary School recognises that social media is an integral part of modern communication and presents both significant opportunities and risks. In line with *Keeping Children Safe in Education (KCSIE) 2024–2025*, online safety, including social media use, is a **core safeguarding priority** and must be a *running and interrelated theme* throughout all school policies, practice and culture.

We are committed to:

- Protecting pupils from online harms arising from social media use, including harmful content, contact, conduct and commerce risks (the 4Cs).
- Ensuring staff, parents and pupils use social media responsibly and safely.
- Upholding the school's reputation online.
- Embedding social media education within the curriculum in line with DfE guidance (*Teaching Online Safety in Schools 2023*).
- Supporting parents to understand social media risks, trends and controls.
- Complying with the **DfE Filtering & Monitoring Standards (2023, updated 2024)** to ensure safe access to digital platforms.

2. Legal and Statutory Framework

The school will ensure compliance with *Keeping Children Safe in Education (KCSIE) 2026* and maintain a whole-school approach to safeguarding, including online safety, site security, filtering and monitoring systems, and staff awareness of emerging risks including AI-generated content, misinformation and cyber-security threats.

KCSIE 2026 emphasises:

- online safety as a whole-school safeguarding responsibility;
- filtering and monitoring systems;
- misinformation and disinformation risks;
- AI-generated content and manipulated imagery;
- DSL oversight of online safeguarding arrangements

Author	Updated	Page
Tracie Langfield	September 2026	2 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

This policy is informed by the following legislation and guidance:

- *Keeping Children Safe in Education 2026* (statutory)
- *Teaching Online Safety in Schools*, DfE (2023) [[assets.pub...ice.gov.uk](#)]
- *DfE Filtering & Monitoring Standards* (2026) [[complaintinfo.com](#)]
- *Prevent Duty Guidance* (Home Office, 2023) [[gov.uk](#)]
- UK GDPR
- Data Protection Act 2018
- Computer Misuse Act 1990
- Management of Health and Safety at Work Regulations 1999 (as amended).
- Equality Act 2010
- **Online Safety Act 2023**

This policy operates alongside:

- Online Safety Policy
- Child Protection & Safeguarding Policy
- Cybersecurity Policy
- Data Protection Policy
- Staff Code of Conduct
- Behaviour & Anti-Bullying Policies
- Acceptable Use Policies (staff, pupils)
- Social Media Code of Conduct for Parents

3. Roles and Responsibilities

Governing Board

- Ensure compliance with KCSIE 2026 requirements for online safety as a core safeguarding risk.
- Ensure filtering and monitoring meet DfE standards and are reviewed **annually**.
- Ensure policies are kept up-to-date with statutory changes.
- Ensure the DSL's remit includes digital safeguarding.

Author	Updated	Page
Tracie Langfield	September 2026	3 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

- Ensure the school complies with DfE filtering and monitoring standards and receives regular assurance reports on their effectiveness.
- Ensure online safety forms part of the school's safeguarding audit programme.

Headteacher

- Oversee implementation of this policy.
- Approve and monitor all school social media accounts.
- Ensure staff are trained in digital safeguarding and reputation management.
- Ensure systems prevent illegal content, deepfakes and AI-generated harmful content (DfE 2024 update).
- Ensure appropriate staff training is delivered regarding AI technologies, emerging online risks and cyber resilience.
- Ensure social media incidents are reviewed as part of safeguarding monitoring.

Designated Safeguarding Lead (DSL)

- Lead responsibility for online safety, including social media risk.
- Understand filtering/monitoring alerts, incidents and risks.
- Respond to reports of online harm, harassment, grooming or radicalisation.
- Identify vulnerable children disproportionately at risk, in line with NSPCC guidance.

Staff

- Maintain professional boundaries online.
- Understand reputational risks and avoid sharing anything that could bring the school into disrepute.
- Never contact pupils via personal social media accounts.
- Report all social media concerns immediately to the headteacher or DSL.

Parents

- Follow the Social Media Code of Conduct.
- Avoid posting images of other children or negative commentary about staff or pupils.
- Engage with training and workshops.

Pupils

- Follow the Pupil Acceptable Use Agreement.

Author	Updated	Page
Tracie Langfield	September 2026	4 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

- Report concerns about social media use affecting themselves or peers.
- Adhere to age restrictions and avoid anonymous or harmful posting behaviours.

5. Cyber Security and Digital safety

KCSIE 2026 strengthens expectations around cyber resilience.

The school will maintain appropriate cyber security arrangements including:

- secure management of devices and networks;
- multi-factor authentication where applicable;
- regular software updates and patching;
- appropriate filtering and monitoring systems;
- annual review of cyber security risks;
- staff awareness training regarding phishing, data security and AI-related risks.

7. School Social Media Accounts

- Only the headteacher may authorise the creation of school social media accounts.
- All accounts must be linked to school-owned emails and stored in secure password vaults.
- At least **two** approved administrators must oversee each account.
- All content must be pre-checked, non-political, inclusive, and compliant with data protection rules.
- No pupil may be individually identified by full name alongside an image.

5. Staff Use of Personal Social Media

Staff must not:

- Use disappearing-message applications to communicate with pupils.
- Use private messaging platforms for school business unless authorised.
- Share confidential school information online.
- Comment publicly on school safeguarding matters.
- Staff must not "friend", follow or interact with pupils or ex-pupils under 18.
- Staff should avoid connecting with parents on personal accounts.
- Privacy settings must be applied to protect personal information.

Author	Updated	Page
Tracie Langfield	September 2026	5 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

- Staff must not post content referencing the school, pupils or colleagues negatively.
- Staff should be aware of digital footprint risks, including misinformation, AI-generated content and identity spoofing (KCSIE 2026).

This reflects current safeguarding expectations and professional conduct standards.

6. Pupil Use of Social Media

- Pupils may not access social media on the school network unless part of a supervised curriculum activity.
- The school's filtering system blocks major platforms, as required under DfE filtering standards.
- Pupils must follow age restrictions for platforms.
- Misuse, cyberbullying or online reputational harm will be managed under the Behaviour and Safeguarding Policies.

7. Data Protection and Consent

The school will process personal data in accordance with UK GDPR and Data Protection Act 2018 principles including lawfulness, fairness, transparency, data minimisation and security.

All official social media platforms must operate using school-controlled accounts rather than personal accounts.

- The school will obtain annual parental consent for the use of pupil images/videos.
- No personal information (full names, contact details) will accompany pupil images.
- Only school devices may be used to take photos/videos.
- Data minimisation strategies (e.g., blurred faces, side facial view) will be used where appropriate.

8. Safeguarding and Social Media Risks

The school will act promptly to protect pupils from:

- Online harassment and bullying
- Grooming, exploitation and coercion
- Sexual harassment and harmful sexual behaviour online

Author	Updated	Page
Tracie Langfield	September 2026	6 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

- Radicalisation and extremist content
- Misinformation, disinformation and conspiracy content (KCSIE 2026 requirement)
- AI-generated impersonation, deepfakes or manipulated images (DfE 2024/25 direction)

All incidents will be logged and acted upon following safeguarding procedures.

9. Social Media Incident Management

The school will maintain procedures for responding to:

- cyberbullying;
- malicious or defamatory posts;
- safeguarding concerns;
- unauthorised publication of images;
- impersonation of pupils or staff;
- account compromise or hacking;
- AI-generated abuse or deepfake content.

Incidents will be logged and investigated in accordance with safeguarding, disciplinary and data protection procedures.

9. Online Safety Act Duties

The school recognises the impact of the Online Safety Act 2023 and is committed to protecting pupils from harmful online content and conduct.

Staff will remain alert to:

- AI-generated content and deepfakes;
- online scams and fraud;
- harmful online challenges;
- misinformation and disinformation;
- online radicalisation;

Author	Updated	Page
Tracie Langfield	September 2026	7 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

- anonymous messaging platforms.

Concerns will be managed through existing safeguarding procedures and escalated to the Designated Safeguarding Lead where appropriate.

9. Filtering, Monitoring and Cybersecurity

Multi-factor authentication (MFA) should be enabled on all school social media accounts wherever available.

Passwords must comply with school cybersecurity requirements and be stored securely.

Access rights must be removed immediately when staff leave the school.

To meet DfE Filtering & Monitoring Standards (2024):

- Filtering prevents access to harmful and illegal content, including extremist and abuse imagery.
- Monitoring identifies concerning digital behaviours.
- Reviews occur **monthly** (technical) and **annually** (governor-level).
- Pupils must not access 3G/4G/5G to bypass school protections.

10. Cyberbullying

Cyberbullying of pupils, staff or parents is strictly prohibited and will be managed under safeguarding, behaviour and disciplinary policies.

11. Training and Education

- Staff will receive regular online safety and social media training, aligned with NSPCC and DfE expectations.
- Social media ethics and digital citizenship are included in computing, PSHE and RHE curricula.
- Parents receive termly guidance and workshops.

Author	Updated	Page
Tracie Langfield	September 2026	8 of 12

Responsible body	Title of policy	
Governing body	Social Media Policy	

12. Monitoring and Review

- This policy will be reviewed annually and immediately following significant legislative, safeguarding or technological developments.
- The next formal review date : September 2027

Responsible body	Title of policy	
Governing body	Social Media Policy	



A

