AYLSHAM LEARNING FEDERATION

SOCIAL MEDIA POLICY

Policy Reference:	DB/JT Social Media Policy	Review Frequency:	1 years
Issue Number:	01 (17.11.27)	Next Review Date:	17.11.2028
Author:	K Garnham		

Ratified by the Governors' Curriculum, Assessment and Attainment Committee on: 17.11.2027

Signed: .....

Chair

Contents

1. Purpose & Scope 1
2. Regulatory & Legal Framework 2
3. Staff Guidelines & Professional Boundaries 2
   3.1 Personal Social Media Use 2
   3.2 Online Recruitment Checks (KCSIE Requirement) 2
4. Official School/Federation Social Media Accounts 3
5. Pupil Expectations & Conduct 3
6. Parents and Carers 3
7. Cyberbullying, Online Harassment & Safeguarding 3
8. Incident Management & Policy Breaches 4

Appendix A: Minimum Age Requirements for Major Social Media & Communication Platforms 4

Appendix B: Important Policy & Safeguarding Notes for Staff & Parents 6

1. Purpose & Scope

This policy provides clear boundaries and guidance on the use of social media to safeguard pupils, protect staff, and maintain the reputation of Aylsham Learning Federation.
This policy applies to:

- **All Staff:** Permanent, temporary, supply, volunteers, governors, and contractors.
- **All Pupils:** Enrolled at Aylsham Learning Federation.

- **Parents / Carers:** Interacting with official school/Federation channels or discussing school/Federation matters online.

Scope: This policy covers official school and Federation accounts, personal social media use that impacts Aylsham Learning Federation community or professional standing, and online safety within the curriculum. This policy should also be read in conjunction with the ICT Acceptable Use Policy as well as the Online Safety Policy.

2. Regulatory & Legal Framework

This policy aligns with statutory guidance and legislation, including:

- **Keeping Children Safe in Education (KCSIE)** (latest statutory guidance)
- **UK General Data Protection Regulation (UK GDPR)** & **Data Protection Act 2018**
- **Education Inspection Framework (Ofsted)**
- **The Equality Act 2010**
- **Computer Misuse Act 1990** & **Malicious Communications Act 1988**
- **Online Safety Act 2023**
- **DfE Statutory Guidance: 'Meeting Digital and Technology Standards in Schools'** (Filtering & Monitoring standards)
- **DfE Guidance: 'Mobile Phones in Schools' (2024)**
- **DfE Guidance: 'Searching, Screening and Confiscation' (2022)**
- **DfE Guidance: 'Teaching Online Safety in School'**
- **Working Together to Safeguard Children (latest statutory guidance)**

3. Staff Guidelines & Professional Boundaries

3.1 Personal Social Media Use

- **Professional Boundaries:** Staff must maintain strict professional boundaries with current and former pupils under the age of 18. Staff must **not** accept or invite current pupils as "friends," "followers," or contacts on personal social media platforms.
- **Communication Channels:** All communication with pupils and parents must take place strictly via official school/Federation channels (e.g., school/Federation email, google classroom, work social media accounts etc).
- **Privacy Settings:** Staff are advised to set personal accounts to high privacy settings and regularly audit their digital footprint.
- **Reputation & Confidentiality:** Staff must not post content that brings Aylsham Learning Federation into disrepute, breaches confidentiality, or makes identifiable references to pupils, parents, or colleagues without authorization.

3.2 Online Recruitment Checks (KCSIE Requirement)

- In line with KCSIE guidelines, Aylsham Learning Federation conducts online searches (including publicly available social media) for shortlisted candidates as part of its due diligence during recruitment.

- Searches strictly target potential safeguarding risks, hate speech, illegal activity, or unprofessional conduct. These checks are carried out in compliance with UK GDPR.

4. Official School/Federation Social Media Accounts
Official school/Federation accounts (e.g., X, Instagram, YouTube) are reviewed centrally to showcase achievements and communicate with the community.

- **Management:** Accounts must be approved by the Executive Headteacher/Headteacher and reviewed by nominated administrators using official school/Federation credentials. Records of log in details must be sent to the Executive Headteacher's/Headteacher's PA for safe keeping using encryption methods. Multi-Factor authentication must be used for all school related social media accounts
- **Pupil Media Consent:** Photos or videos of pupils will **only** be published if consent has been granted by parents/carers.
- **Identification Rules:** Full names of pupils will **not** be published alongside photos unless explicit consent is obtained.
- **Moderation:** Account admins will actively monitor comments and disable public commenting where appropriate to prevent trolling or spam.

5. Pupil Expectations & Conduct
Pupils are expected to demonstrate responsible digital citizenship, both on and off school premises.

- **Banned Behaviour:** Cyberbullying, harassment, targeted insults, impersonation of staff or peers, sharing non-consensual imagery (including deepfakes or altered images), and creating social media pages targeting Aylsham Learning Federation are strictly prohibited.
- **Mobile Devices:** Mobile phone use on school premises must adhere to Aylsham Learning Federation's behaviour expectations around Mobile Phones. Each school within the Federation may have their own behaviour expectations around Mobile Phone use within each school's setting.
- **Reporting:** Pupils are encouraged to report any instances of online abuse, inappropriate content, or pressure experienced online to a Designated Safeguarding Lead (DSL) or a trusted member of staff.

6. Parents and Carers

- **Positive Community Standard:** Parents/carers are encouraged to use official school communication channels for concerns or complaints rather than public social media groups.
- **Event Media:** Parents taking photos or videos at open events (sports days, school plays etc) must use them for **personal use only** and must not upload identifiable images of other people's children to social media without consent.

7. Cyberbullying, Online Harassment & Safeguarding
Aylsham Learning Federation treats cyberbullying with the same severity as offline bullying.

Risk Area	School Response / Procedure
Child-on-Child Abuse	Investigated immediately under the Safeguarding and Anti-Bullying Policies. Involves the DSL and parents.

Risk Area	School Response / Procedure
Generative AI & Deepfakes	Creating or distributing AI-generated explicit/harmful images or text targeting pupils or staff is treated as a major safeguarding breach and may involve the police.
Misinformation & Extremism	Social media content promoting radicalisation, hate speech, or dangerous illegal challenges will be escalated immediately to a DSL under Prevent duties.

8. Incident Management & Policy Breaches

Breaches of this policy will be dealt with promptly under relevant Federation policies:

1. **Staff Breaches:** May result in disciplinary action up to and including gross misconduct dismissal, referral to the Teaching Regulation Agency (TRA), or reporting to the Disclosure and Barring Service (DBS).
2. **Pupil Breaches:** Handled via Aylsham Learning Federation Behaviour Policy, ranging from internal sanctions and loss of technology privileges to suspension or permanent exclusion. Legal authorities will be involved where criminal activity (e.g., malicious communications, non-consensual image sharing) is suspected.
3. **Takedown Requests:** Aylsham Learning Federation will formally request the removal of defamatory, illegal, or abusive content from social media platforms and, where necessary, seek legal remedies.

Appendix A: Minimum Age Requirements for Major Social Media & Communication Platforms

This appendix sets out the minimum age requirements established by popular social media networks, messaging apps, and online gaming platforms. Under the UK General Data Protection Regulation (UK GDPR), children under the age of 13 cannot give their own consent for processing personal data on online services, which underpins the default baseline age for most platforms.



Platform Age Matrix

Platform	Minimum Age Limit	Key Safeguarding Notes & Parental Controls
TikTok	**13+**	Accounts for users aged 13–15 are set to **Private** by default. Direct messaging is disabled for users under 16, and live streaming is restricted to 18+.
Instagram	**13+**	Accounts for under-16s default to private. Instagram includes Teen Account restrictions that limit sensitive content and restrict direct messaging from unknown users.
Snapchat	**13+**	Under-18s receive additional safety prompts when contacted by strangers. Location sharing via "Snap Map" is turned off by default for minors.
WhatsApp	**13+**	*(Lowered from 16 to 13 in the UK/EU in April 2024 to align with global standards).* Parents can manage privacy settings to control who can add pupils to group chats.
Discord	**13+**	Certain user-created servers contain age-restricted (18+) content filters. Default privacy settings require friends-only direct messaging for younger users.

Platform	Minimum Age Limit	Key Safeguarding Notes & Parental Controls
X (formerly Twitter)	**13+**	Content filters must be manually set. Under-18s cannot register for premium monetized features or altered account types.
YouTube	**13+**	Users aged 13–17 require parental permission or supervision via Google Family Link to set up standard channels. (YouTube Kids is intended for under-13s).
Reddit	**13+**	Subreddits marked as NSFW (Not Safe For Work) are age-gated to 18+. Account settings allow users to disable adult content feeds.
Twitch	**13+**	Streamers and viewers aged 13–17 must have permission from a parent or legal guardian to stream or interact in live chats.
Facebook	**13+**	Privacy settings restrict targeted advertising to under-18s based on age and location only.
Kick	**13+**	Requires parent/guardian consent for users aged 13–17. Unfiltered live streams make moderation critical.
BeReal / Yubo	**13+** *(BeReal & Yubo)*	**Yubo** operates separate communities for teens (13–17) and adults (18+) to prevent inter-age contact.
Minecraft	**7+**	Users can play single player (not online) or multiplayer (access to online worlds and chats). Depending on whether playing on an Xbox or a PC/Tablet/Phone depends on whether parental controls are managed through your Microsoft Xbox account or need setting up separately.
Roblox	**5+**	Certain aspects of the app are disabled at particular ages and are only unlocked when a user hits a certain age

Appendix B: Important Policy & Safeguarding Notes for Staff & Parents

1. **Age Verification & UK Online Safety Act:** The UK Online Safety Act requires platforms to enforce robust age-checking mechanisms (e.g., facial age estimation, photo ID verification) to protect children from age-inappropriate content.

2. **Under-Age Account Usage:** Pupils using platforms below the specified minimum age are doing so in breach of the platform's Terms of Service. If an under-age account is reported in connection with school-related bullying or safeguarding concerns, Aylsham Learning Federation will escalate the issue to parents/carers and request account deletion via the platform's safety center.
3. **Data Protection & Parental Responsibility:** For any platform accessed by a pupil under the age of 13, legal consent for data harvesting rests with the parent/guardian. Staff members must never encourage or assist a pupil under the legal age limit in creating an account.