Burstwick Community Primary School

School Social Media Management Policy

Complete these fields	School entry
School / trust	Burstwick Community Primary School
Approved by / date	Governing Body
Effective from	01/09/2026
Review date	31/08/2027

A simple safeguarding-first policy for school-managed channels

"BURSTWICK: Small School. Big Hearts. Where Learning Comes Alive."

At Burstwick Community Primary School, our children thrive, develop and master their independence and confidence in a busy and enthusiastic learning environment.

Within our school, our children have a strong voice, feel cared for, supported and are part of the Burstwick family.

At Burstwick Community Primary School, we live by our core values. These values support the development of the whole child as a reflective learner within an enthusiastic and focused atmosphere.

***CORE VALUES: B**elievers, **U**nique, **R**esilient, **S**afe, **T**olerant, **W**orthy, **I**ndependent, **C**reative, **K**ind-hearted.*

*We are **BURSTWICK!***

Policy at a glance

The school uses social media to communicate useful information and celebrate school life. It will do so without exposing pupils, staff or families to avoidable safeguarding, privacy or reputational risk.

> **CORE RULE** Safeguarding and dignity come before publicity, convenience or engagement. If anything is unclear, do not post until it has been checked.

1. **Public pupil images.** The school will no longer publish clear, front-facing or otherwise readily identifiable pupil faces on public social media or the public website.
2. **Names and identifiers.** The school will no longer a pupil image with a name, voice, class, location, certificate or other detail that identifies them unnecessarily.

3. **Permission and lawful basis.** The school will check the school's current record before use. Permission does not replace the need for a lawful basis and clear privacy information.
4. **Pupil choice.** The school will respect a pupil who does not want to be photographed, filmed or published for promotional purposes, even where adult permission exists.
5. **Closed platforms.** Identifiable faces may be used only on an approved, authenticated parent platform under the separate rules in section 4.
6. **Devices.** The school will only use school-owned or formally managed devices and storage only. Personal phones, accounts and cloud storage must not be used for pupil content.
7. **Direct messages.** Staff will never conduct private social media conversations with pupils.
8. **Accounts.** The school will always use multi-factor authentication, at least two trained administrators and managed recovery details.
9. **Safeguarding.** The school will report any disclosure, allegation, harmful contact or sexual imagery to the DSL immediately.
10. **Stop rule.** If safety, permission, accuracy, approval, accessibility or copyright is uncertain, The school will not post.

1. Purpose and scope

This policy sets the rules for creating, approving, publishing, monitoring and removing content on the school's official social media channels. It also applies when the same team supplies content to the public website or publishes photographs and video through an authenticated parent platform.

It applies to all employees, governors, trustees, volunteers, agency staff, contractors and any other person authorised to create, supply, approve, schedule, publish, moderate, download or store official content.

Official channels include Facebook, Instagram, Threads, LinkedIn, YouTube, TikTok, X and any similar service approved in the school's name. Staff will never create a school, class, club or department account without written Headteacher approval.

1.1 Related policies

This policy must be read with the school's:

* Child Protection and Safeguarding Policy,

* Staff Code of Conduct,

* Data Protection Policy and privacy notices,

* Acceptable Use Policy,

* Complaints Policy,

* Retention schedule and;

* any trust or local-authority communications rules.

Safeguarding and applicable law take priority if policies conflict.

2. Responsibilities

Role	Responsibility
Governing body / trust board / proprietor	Approve the policy and receive assurance that suitable safeguarding, data protection and security controls are in place.
Headteacher	Approve official channels and high-risk content; appoint the Social Media Lead; ensure the policy is followed.
DSL	Advise on pupil risk and do-not-publish restrictions; lead safeguarding incidents and external referrals.
Data Protection Officer (DPO)	Advise on lawful basis, privacy information, DPIAs, rights, retention, platforms and personal data breaches.
Social Media Lead	Manage channels, permissions checks, approvals, moderation, account access, records and routine reviews.
All contributors	Use approved devices and storage, follow this policy, check content carefully and report concerns immediately.

In a small school, one person may hold more than one operational role. Sensitive or high-risk content will still be checked by an appropriate second person.

3. Data protection and permission

An identifiable photograph, video, voice recording, name, comment or message is personal data. A pupil may still be identifiable when their face is hidden because of their voice, uniform, name, class, wheelchair, distinctive clothing, location, caption or the context of the post.

The school will document a lawful basis for each material use of personal data. Relevant bases may include public task, legitimate interests or consent, depending on the school's status, purpose and circumstances. The DPO will confirm the approach. The school will not state that permission alone makes processing lawful.

3.1 Privacy information, permission and objections

11. The school will tell pupils, parents, carers and staff what will be used, why, where it may appear, who may receive it, how long it is kept, the risks of public platforms and how to object or withdraw consent.

12. The school will keep a clear, current record of permission, consent, restrictions, objections and withdrawals. Check it again before publication because circumstances can change after a photograph is taken.
13. Where consent is the lawful basis, it must be freely given, specific, informed, unambiguous, recorded and as easy to withdraw as to give.
14. Where another lawful basis is used, offer a clear permission or opt-out process where possible and consider objections fairly. **An opt-out is not the same as UK GDPR consent**.
15. The school will explain the intended use to the pupil in suitable language. Respect refusal or discomfort for promotional content and provide an inclusive alternative so the pupil is not disadvantaged.
16. The school will send rights requests and data-protection complaints to the DPO immediately. The school will provide an electronic complaint route, acknowledge a data-protection complaint within 30 days and respond without undue delay.

LIMIT OF CONTROL: The school can remove content from accounts it controls, but cannot guarantee recall of copies already downloaded, screenshotted, scraped, indexed, reshared or retained by a platform. This must be made clear before public publication.

4. Pupil photographs and video

4.1 Public social media and website

The school will no longer publish clear, front-facing or otherwise readily identifiable pupil faces on public channels. This is a safeguarding and data-minimisation measure. It does not remove the need to check the lawful basis, permission and wider context where a pupil can still be identified.

17. The school will use back-of-head, over-the-shoulder, hands-at-work, detail, wide environment and outcome-focused photographs.
18. The school will check mirrors, reflections, certificates, books, screens, labels, lanyards, medical details, vehicle registrations, geotags and background information.
19. The school will no longer publish a pupil's full name. The school will not combine a first name or initials with an image, voice, class, award, exact location or other information that identifies them, unless an exceptional use has been specifically approved by the Headteacher, DSL and DPO.
20. The school will not tag pupils, link to their accounts, invite the public to identify them or repost a parent's content merely because it is already public.
21. The school will not publish real-time pupil locations, routes, accommodation, timetables or information that exposes site security or reduced staffing.

4.2 Content that must not be published

The school will not publish a pupil where the DSL has recorded a safeguarding restriction, court order, adoption or care-related risk, refuge or witness-protection concern, custody dispute or other reason why identification may cause harm. Staff checking a post need only know the publish or do-not-publish result, not the confidential reason.

The school will not publish pupils in toilets, changing areas, intimate care, medical treatment, distress, restraint, disciplinary situations, sleepwear or swimming attire, or in content that could humiliate, sexualise, stereotype or expose vulnerability. The school will not identify an individual through posts about SEND, health, behaviour, attendance, poverty, family circumstances or safeguarding.

4.3 Closed parent platforms

Identifiable pupil faces may be used on a closed parent or learning platform only if the platform has been approved, the DPO has completed the required risk assessment or DPIA, access is authenticated and restricted, the lawful basis and privacy information are clear, and the school's separate closed-platform permission has been checked. For this purpose, the school uses only DOJO, and consent has been given by parents/carers.

22. Use the smallest appropriate audience, such as the relevant parent or class group rather than the whole school.
23. Remove access promptly when a pupil leaves or an adult's relationship or role changes.
24. Apply the same dignity, safeguarding and sensitive-information rules as for public content.
25. Disable public links, unnecessary downloads, onward sharing, comments and direct messages where the platform allows.
26. Tell families not to copy or repost images of other children, while being honest that technical controls cannot make copying impossible.

SEPARATE DECISION Seesaw, Tapestry, ClassDojo and similar services are not automatically approved or risk-free. Public social media permission and closed-platform permission must be kept as separate choices.

5. Capturing, editing and storing content

27. The school will use school-owned or centrally managed cameras, phones, tablets, memory cards and computers. Personal devices and personal cloud storage are prohibited for pupil content.
28. The school will disable personal photo-library sync, automatic uploads to unapproved services and location tagging.

29. The school will transfer content to approved school storage by the end of the working day. The school will check the transfer, then delete the device and memory-card copy.
30. The school will limit source-folder access to staff who need it. The school will not send pupil media through personal email, consumer messaging apps or unapproved removable media.
31. The school will not upload pupil images, video, voice, names, safeguarding information or confidential school content to a public AI, face-editing, captioning or image-enhancement service.
32. The school may consider using an AI or automated tool only after DPO and IT approval, supplier checks and a DPIA where required. The school will not use facial recognition, emotion analysis or profiling for social media content.

6. Content and approval

Official content must be accurate, necessary, proportionate, respectful, inclusive, accessible and consistent with the school's values. It must use plain English and an official contact route. Scheduled content must be checked again if circumstances change before publication.

Level	Examples	Approval
Routine	Dates, reminders, vacancies, buildings, displays and content with no personal data	Social Media Lead after checklist
Pupil-related	Any pupil image, voice, work, group, award, trip or performance, including no-face imagery	Permission check and Social Media Lead
Sensitive / high-risk	Safeguarding, health, SEND, crisis, allegation, complaint, live stream, political issue, paid targeting, new platform or AI use	Headteacher plus DSL, DPO, IT or trust / LA advice as relevant

6.1 Do not publish

33. Confidential, medical, SEND, behaviour, attendance, safeguarding, assessment or family information about an identifiable person
34. Unverified claims, rumours, allegations or information that could prejudice an investigation or court process
35. Content that embarrasses, ridicules, stereotypes, shames or places pressure on a child or adult
36. Party-political campaigning or unbalanced presentation of political issues where impartiality duties apply

37. Commercial endorsements, competitions, sponsorships or fundraising claims without approval and clear disclosure
38. Photographs, video, music, logos, artwork, screenshots, quotations or pupil work without verified rights and permission
39. Security details, access codes, staff absences, real-time pupil movements or site vulnerabilities

7. Accounts, comments and direct messages

7.1 Account security

40. The school will use an official school email and organisational account-management tools. No account may depend on one employee's personal profile, phone number or recovery email.
41. The school will have at least two trained administrators, with one senior owner. Give each person the lowest access needed.
42. The school will enable multi-factor authentication, use unique passwords in the approved password manager and record all connected scheduling or analytics tools.
43. The school will review users, roles, recovery details, connected apps and security alerts at least termly. The school will remove access before or on a person's last working day and immediately where misuse is suspected.

7.2 Comments and messages

44. The school will monitor comments, mentions, tags and inboxes on active working days, with planned cover for absence and holidays.
45. The school will not discuss or disclose case details, or investigate complaints publicly. The school will acknowledge briefly and direct the person to the official complaints route.
46. The school will hide, delete, report or restrict content that identifies or targets a child, shares personal data, threatens, discriminates, harasses, defames, breaks the law, is spam or breaches the platform rules. Fair criticism must not be removed merely because it is negative.
47. The school may use direct messages for confidential information, safeguarding, formal complaints, absence reporting or emergencies, and this will be recorded using the school preferred management system CPOMS.
48. Staff will not follow, friend or privately message current pupils from official or personal accounts. If a pupil messages an official account, do not continue a private conversation. Pass it to the DSL and use only the minimum response needed to keep the pupil safe.

8. Safeguarding, mistakes and breaches

Any online content or contact suggesting abuse, exploitation, grooming, self-harm, suicide risk, bullying, radicalisation, criminal exploitation, a missing child, an allegation against an adult or another safeguarding concern must be reported to the DSL immediately and handled under the Child Protection and Safeguarding Policy. Call 999 if anyone is in immediate danger or a crime is in progress.

SEXUAL IMAGERY: The school will never view, copy, print, screenshot, share, store, save or ask a child to download or forward nude or semi-nude imagery. The school will report it to the DSL immediately. If it has been viewed accidentally, the school will stop and tell the DSL exactly what happened. Only the DSL or delegated safeguarding lead may decide whether viewing is necessary under national guidance.

8.1 Wrong post, account compromise or personal data breach

49. **Contain.** The school will remove, unpublish or restrict the content where safe; disable scheduling; revoke unauthorised access; ask IT to secure the account and preserve logs.
50. **Tell the right people.** The school will notify the Headteacher, Social Media Lead, DPO, DSL and IT according to the incident. Do not wait for certainty.
51. **Record.** The school will note what happened, discovery time, audience, people affected, known copies or shares, containment and decisions. The school will not create a copy of illegal sexual imagery.
52. **Assess and notify.** The DPO decides whether the ICO and affected people must be notified. A notifiable breach must be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness.
53. **Learn.** The school will correct public information, reset security, support affected people, document lessons and update training or controls.

9. Live content, accessibility, copyright and retention

9.1 Live and real-time content

The school will not live stream pupils on public social media, although DOJO is a closed approved group and an exception to this. Any exception needs a written event risk assessment and approval from the Headteacher, DSL and DPO, with current permission, controlled camera zones, active moderation and a tested way to stop the stream. Edited highlights are preferred.

The school will not post school trips, residentials, fixtures or pupil movements in real time where this exposes a precise location, route, accommodation, room, timetable or site-security risk.

9.2 Accessibility

54. The school will not make important information available only through social media. The school will use an accessible official route such as the website, email, parent system or telephone service.
55. The school will use readable contrast, clear fonts, sentence case, short paragraphs, descriptive links and CamelCase for multi-word hashtags.

9.3 Copyright and advertising

56. The school will publish only content the school owns, is licensed to use for that platform and purpose, or may lawfully use under a documented exception. Credit does not replace permission.
57. The school will does not assume music in a platform's library is licensed for a school, organisational, advertising or cross-platform use. The school will check the terms and any separate licence.
58. The school will not upload pupil, parent, carer or staff contact lists to an advertising platform, create custom audiences from school records, or install tracking pixels without written DPO and Headteacher approval.

9.4 Recommended retention

Asset	Recommended default
Device / memory-card copy	Delete immediately after verified transfer, and no later than the end of the working day.
Unselected or duplicate identifiable source media	Delete once selection is complete, normally within 30 days.
Selected identifiable working media	Delete by the start of the following term unless a continuing purpose is recorded.
Non-identifiable reusable assets	Review after 12 months.
Closed-platform content	Follow the educational purpose, platform settings and approved school retention schedule.
Permission, approval and incident records	Keep under the school's approved data protection, safeguarding and records-retention schedules.

Delete content sooner after a valid withdrawal, upheld objection, safeguarding restriction, expiry of purpose or material error. Do not delete records subject to a safeguarding hold, complaint, investigation, legal claim, information request or police instruction without advice.

10. Introducing this policy

Where the school is moving away from publishing identifiable pupil faces publicly, it will:

59. **Set the date and scope.** The school will record which public channels are changing and the separate position for closed parent platforms.
60. **Update the paperwork.** The school will consult with the DPO to check the privacy notice, lawful bases and permission categories. Fresh consent is not automatically required merely because public identification is being reduced. The school will obtain it where consent is the lawful basis and the existing wording no longer covers the purpose, platform, audience or risks.
61. **Inform parents and pupils.** The school will explain that the change is preventive and safeguarding-led, what will still be published and how closed platforms differ.
62. **Audit historic content.** The school will prioritise clear faces, names with images, certificates, vulnerable pupils, real-time locations, widely shared posts and items raised as a concern.
63. **Train and align.** The school will show staff practical no-face photography, the permission check, device rules and escalation route. Align the website, photo, mobile-device and staff guidance.

> **WHY TELL PARENTS?** A visible change should be explained calmly so families understand the preventive safeguarding reason and do not assume a specific incident has occurred.

11. Monitoring and review

64. The Social Media Lead monitors active channels and checks account access, settings, connected apps and the permissions process at least termly.
65. The DSL and DPO review their relevant controls after an incident and as part of the annual policy review.
66. The policy is reviewed at least annually, and sooner after a material legal or guidance change, new platform, serious error, safeguarding concern, breach or complaint trend.
67. Concerns or removal requests should be sent to the school email address – burstwickcommunity.primary@eastriding.gov.uk. Safeguarding concerns go to the DSL; data-protection complaints and rights requests go to the DPO; general complaints follow the school's complaints procedure.

Safeguarding

The school is committed to safeguarding and promoting the welfare of all children and staff. We expect all staff and volunteers to share this commitment. Through the construction and writing of policies, we share our commitment; and through our curriculum provision, safeguarding is taught both explicitly (directly) and implicitly (indirectly).

We believe that all children have the right to learn in a supportive, caring and safe environment, which includes the right to protection from all types of abuse. Staff are vigilant for signs of any child in distress and we are confident about applying our safeguarding procedures to avert and alleviate any problems.

Monitoring and Review

Burstwick Community Primary School's School Media Management Policy is monitored regularly by the Senior Leadership Team (SLT), DSL, DPO, and E-Safety Coordinator, who report to the governors about its implementation and effectiveness. Governors are kept informed of any significant changes via the termly Headteacher's Report.

This Policy will be reviewed at least once every two years as a minimum, or if directives dictate change, through discussion with all staff and Governors.

Headteacher: ***Ian Cutts***	Chair of Governors: ***Andy Johnson***
Signed:	Signed:

Appendix A. One-page pre-post check

The publisher must be able to tick every applicable box. If not, stop and ask.

- ☐ There is a clear school purpose and this is the least intrusive way to achieve it.
- ☐ The channel and publisher are authorised.
- ☐ The current permission, objection and confidential do-not-publish check is complete.
- ☐ No pupil is unnecessarily identifiable from a face, name, voice, uniform, caption, class, location or background detail.
- ☐ The pupil is comfortable and has not objected.
- ☐ Facts, dates, names, links, contact details, captions and claims are accurate.
- ☐ The correct person has approved the post and the approval is recorded.
- ☐ The post reveals no live pupil movement, access detail, staff absence or site-security information.
- ☐ Key information is accessible, with useful alt text, checked captions and an alternative official route where needed.
- ☐ The school owns or has permission and the correct licence for every image, clip, track, logo, artwork and quotation.
- ☐ The wording is respectful, inclusive, impartial and suitable for a public audience.
- ☐ The asset is in approved storage and has a review or deletion point.
- ☐ Nothing has changed since approval that makes a scheduled post unsafe or inaccurate.

FINAL QUESTION Would we be comfortable explaining this post, its purpose and our checks to the pupil, their family, the governing body, the local authority or trust, and the Information Commissioner's Office? If not, do not publish it.

Appendix B. Legal framework and current guidance

This policy is designed to support compliance with the following framework in England. It was checked against the linked primary and regulator sources in June 2026. The school should use current versions at each review.

Framework	Why it matters
UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025	Lawfulness, fairness, transparency, minimisation, security, retention, accountability, rights and complaint handling.
Education Act 2002 and Children Acts 1989 and 2004	Safeguarding and promoting children's welfare.
Keeping Children Safe in Education	KCSIE 2025 applies until 31 August 2026. KCSIE 2026 applies from 1 September 2026.
Equality Act 2010 and accessibility requirements	Inclusive communication, reasonable adjustments and accessible digital information.
Copyright, Designs and Patents Act 1988	Rights in photographs, video, music, writing, artwork, logos and pupil work.
Education Act 1996 sections 406 and 407	Political impartiality and balanced treatment of political issues where applicable.

DfE: Taking and using photos and videos in schools

ICO: Taking photographs - data protection advice for schools

ICO: Data sharing and children

ICO: Data (Use and Access) Act 2025 - what it means for organisations

DfE: Keeping Children Safe in Education

UKCIS / DfE: Sharing nudes and semi-nudes

DfE: Cyber security core standard

ICO: Personal data breaches - a guide

GOV.UK: Accessibility requirements for public sector websites and apps

Intellectual Property Office: Digital images, photographs and the internet