



APPLEFORD SCHOOL SOCIAL MEDIA POLICY

This policy, which applies to all staff, volunteers, contractors and visitors working with pupils in education or the boarding provision publicly available on the school website, on the staff share and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. This policy reflects current legislation, the social media duties and emerging DfE, ISI and Ofsted SCCIF expectations for residential special schools

We have a whole school approach to safeguarding, which is the golden thread that runs throughout every aspect of the school. All our school policies support our approach to safeguarding (child protection). Our fundamental priority is our children and their wellbeing; this is first and foremost.

This policy applies in:

- classrooms and learning spaces;
- residential accommodation and during boarding routine;
- on-site and off-site activities, including trips, transport and work experience.

Legal and regulatory framework: This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including the requirements for lawful processing and consent in relation to photographs, video and other personal data shared on social media (updated June: 2026);
- the statutory guidance “Keeping Children Safe in Education” (KCSIE 2026), including expectations around staff conduct online, safer recruitment (including online searches of shortlisted candidates), and managing allegations against staff;
- the Teachers' Standards, Part 2, which sets out expectations of personal and professional conduct, including online, that apply both in and outside school;
- the Protection from Harassment Act 1997, the Malicious Communications Act 1988 and section 127 of the Communications Act 2003, which create criminal offences relating to harassment and the sending of grossly offensive, indecent or menacing communications;
- the Defamation Act 2013, in respect of the risk of defamatory statements made online;
- the Equality Act 2010, in respect of online harassment or discrimination connected to a protected characteristic;
- guidance from the Information Commissioner's Office (ICO) on social media and data protection;
- the Counter-Terrorism and Security Act 2015 (the “Prevent duty”), insofar as it relates to identifying and responding to extremist or radicalising content encountered on social media; and
- the Independent School Standards (ISS) and the Ofsted SCCIF currently in force

This policy operates in conjunction with the following school policies:

- | | |
|---|---|
| • Keeping Children Safe in Education (currently in force) | • Complaints Policy |
| • Child Protection and Safeguarding Policy | • Recruitment and Safer Recruitment Policy |
| • Online Safety Policy | • Social Media Code of Conduct for Parents |
| • Cyber Security Policy | • Device and Technology Acceptable Use Agreement for Staff |
| • Data Protection Policy and Privacy Notices | • Device and Technology Acceptable Use Agreement for Pupils |
| • Staff Behaviour Policy (Staff Code of Conduct) | • Complaints Procedures |
| • Anti-Bullying (Countering Bullying) Policy | • Low-level Safeguarding Concerns Policy |
| • Behaviour Policy | • Confidentiality Policy |
| • Mobile Phone Policy | • Disciplinary Policy and Procedure |
| • Prevent Duty Risk Assessment | • School Social Media Accounts – Terms of Use Agreement |
| • Photography and Image Consent Policy | |

Monitoring and Review: The text of this policy is necessary and proportionate to meet the needs of Appleford School, supporting those who work with our pupils, making clearer the responsibilities of school staff, volunteers, proprietor and the Advisory Board. This policy is designed to support the Appleford School staff who work with our pupils who have special educational needs and disabilities (SEND) making clearer the responsibilities of school staff, and the proprietor. These arrangements are subject to continuous monitoring, refinement, and audit by Dr Peter Gardner (Proprietor and Managing Director), and Mr David King (Headmaster and Non-Executive Director).

The Proprietor Headmaster and Designated Safeguarding Lead will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented, or sooner in response to a significant incident or a change in relevant legislation or statutory guidance. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements, and it will be made available to them in writing or electronically.

Policy reviewed, agreed and published: September 2026

Next review: September 2027

Signed



Dr Peter Gardner
Proprietor and Managing Director

Mr James Langan
Headmaster

Statement of intent

Induction, purpose, and scope

Appleford understands that social media is a growing part of life outside of school. Social media offers Appleford valuable opportunities to celebrate pupils' achievements, share school news, and engage with our school community. It also carries risks, including safeguarding risks, data protection risks, and reputational risks, which must be carefully managed. Younger pupils at this school are advised not to use social media independently, since most platforms set a minimum age requirement of 13. Older pupils, particularly at Key Stage 3 and 4, are likely to hold personal social media accounts outside school, and this policy sets out the standards expected of them, in addition to the school's official use of social media and the conduct expected of staff online.

This policy sets out how Appleford uses social media responsibly, the standards expected of staff, Proprietor, advisory board, volunteers and pupils, and the school's expectations of parents/carers in relation to social media use connected with the school. It should be read alongside the Safeguarding and Child Protection Policy, Online Safety Policy, Cyber Security Policy, Data Protection Policy, Staff Code of Conduct, Anti-Bullying Policy and Behaviour Policy

References to "social media" in this policy include social networking sites, blogs, video and photo-sharing platforms, messaging apps with social or public-facing features, and any other online platform that allows users to create and share content or interact publicly or semi-publicly.

This policy applies to all staff (including teaching, non-teaching, supply and agency staff), advisory board, volunteers and contractors, to all pupils, and to parents/carers in respect of conduct connected with the school. It covers:

- the school's official social media accounts and any content posted on them;
- personal use of social media by staff, advisory board, and volunteers, to the extent that it touches on the school, its pupils, staff, or community;

- personal use of social media by pupils, to the extent that it touches on the school, its pupils, staff, or community, including where this happens outside school hours or off the school site but affects relationships or welfare within the school; and
- the use of photography, video and audio recording in connection with school activities, where this may subsequently be shared on social media

We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- encouraging the responsible use of social media by all staff, parents and pupils in support of the school's mission, values and objectives.
- protecting our pupils from the dangers of social media.
- preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- protecting our staff from cyberbullying and potentially career damaging behaviour.
- arranging online safety meetings for parents.

Roles and responsibilities

The proprietor is responsible for:

- holding strategic oversight of the school's use of social media, approves this policy, and receives an annual report on official account activity, complaints and incidents;
- ensuring this policy is implemented by the school;
- reviewing this policy on an annual basis;
- ensuring the DSL's remit covers online safety
- ensuring their own knowledge of social media and online safety issues is up-to-date;
- ensuring all staff undergo safeguarding and child protection training, including online safety, at induction;
- ensuring that this policy, as written, does not discriminate on any grounds, including against any of the protected characteristics, as outlined in the Equality Act 2010.

The headmaster will be responsible for:

- the school's social media presence and for staff conduct online, and authorises any new official school social media account;
- the overall implementation of this policy and ensuring that all staff, parents and pupils are aware of their responsibilities in relation to social media use;
- promoting safer working practices and standards with regards to the use of social media;
- establishing clear expectations of behaviour for social media use;
- in conjunction with the proprietor, handling complaints regarding this policy and its provisions in line with the school's complaints procedure for data protection;
- implementing appropriate sanctions and disciplinary methods where there is a breach of this policy;
- taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use and
- The headmaster is the DPO and will work alongside the ICT technicians to ensure appropriate security measures are implemented and compliance with UK GDPR and other data protection legislation.

The Designated Safeguarding Lead (DSL) will be responsible for:

- leading the response to any safeguarding concern arising from social media use, including concerns about staff-pupil contact or inappropriate content involving a pupil;
- the school's approach to online safety and
- dealing with concerns about social media use that are safeguarding concerns.

The Data Protection Officer (DPO) will be responsible for:

- advises on the data protection implications of posting images or information online, and oversees compliance with consent and retention requirements;

Staff members will be responsible for:

- adhering to the principles outlined in this policy and the Device and Technology Acceptable Use Agreement for Staff;

- maintaining professional boundaries online at all times, do not contact pupils or accept contact from pupils via personal social media accounts, and report any concern about social media use to the DSL or Headmaster;
- ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom;
- reporting any social media misuse by staff, pupils or parents to the headmaster immediately and
- attending any training on social media use offered by the school.

Parents/Carers will be responsible for:

- follow the school's guidance on the use of social media in relation to the school, including in respect of photographs of other pupils and respectful conduct towards staff and the school community;
- adhering to the principles outlined in this policy and the Social Media Code of Conduct for Parents;
- taking appropriate responsibility for their use of social media and the influence on their children at home;
- promoting safe social media behaviour for both themselves and their children and
- attending meetings held by the school regarding social media use wherever possible.

Pupils will be responsible for:

- Key Stage 2 pupils are advised not to hold personal social media accounts and do not use social media as part of school activities other than through school-managed, staff-supervised channels. Key Stage 3 and 4 pupils, who may hold personal social media accounts outside school, are expected to use them responsibly and respectfully towards the school community, and to follow the Pupil Acceptable Use Policy in respect of any school-related online conduct;
- adhering to the principles outlined in this policy and the Pupil Code of Conduct;
- ensuring they understand how to use social media appropriately and stay safe online;
- seeking help from school staff if they are concerned about something they or a peer have experienced on social media;
- reporting incidents and concerns relating to social media in line with the procedures within this policy and
- demonstrating the same high standards of behaviour as expected within the school.

The marketing/Communications Lead will be responsible for:

- manages the school's official social media accounts, moderates comments, and ensures content is accurate, appropriate and compliant with this policy before publication;
- monitoring and reviewing all school-run social media accounts;
- vetting and approving individuals who wish to be 'friends' or 'followers' on the school's social media platforms;
- consulting with staff on the purpose of the social media account and the content published;
- maintaining a log of inappropriate comments or abuse relating to the school;
- handling inappropriate comments or abuse posted on the school's social media accounts, or regarding the school.
- creating a terms of use agreement, which all content published must be in accordance with and
- ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.

ICT technicians will be responsible for:

- providing technical support in the development and implementation of the school's social media accounts;
- implementing appropriate security measures as directed by the headmaster and
- ensuring that the school's filtering and monitoring systems are updated as appropriate.

Official School social media accounts

Appleford may maintain official social media accounts to share school news, celebrate pupils' achievements, and communicate with the wider school community:

- any new official account must be approved in advance by the Headmaster, who will maintain a register of all official accounts (Appendix A);
- only staff explicitly authorised by the Headmaster may post on behalf of the school, and account passwords/credentials are managed securely in line with the Cyber Security Policy;
- content is reviewed before posting to ensure it is accurate, appropriate, and does not identify a pupil by name alongside their image, or disclose any personal or sensitive information, without the necessary consent;

- no pupil's photograph or video is posted on an official account unless parental consent has been obtained and recorded in line with the Data Protection Policy, and the family's consent preferences are checked before each use;
- comments on official accounts are moderated; the school will not engage in public arguments or disputes online, and any complaint or concern raised via social media is redirected to the school's Complaints Policy rather than addressed in a public comment thread and
- official accounts are reviewed at least annually to confirm they remain appropriate, secure and in active, authorised use.

Social media accounts for the school will only be created by the marketing officer and other designated staff members, following approval from the headmaster. A school-based social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account.

When setting up a school social media account, consideration will be given to the following:

- The purpose of the account
- Whether the overall investment will achieve the aim of the account
- The level of interactive engagement with the site
- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the account
- How the success of the account will be evaluated

The headmaster will be responsible for authorising members of staff and any other individual to have admin access to school social media accounts. Only people authorised by the headmaster will be allowed to post on the school's accounts.

Passwords for the school's social media accounts are stored securely [on the school's ICT network](#). The passwords are only shared with people authorised by the headmaster.

All posts made to school social media accounts will not breach copyright, data protection or freedom of information legislation.

The school's social media accounts will comply with the platform's rules. The marketing officer will ensure anyone with authorisation to post on the school's social media accounts are provided with training on the platform and the rules around what can be posted.

School social media accounts will be moderated by the marketing officer or another designated member of staff.

Staff conduct

Only staff with authorisation from the headmaster will post on school accounts and they will adhere to the School Social Media Accounts – Terms of Use Agreement.

Staff will get content approved by the marketing officer before it is posted. Staff will only post content that meets the school's social media objectives, including the following:

- Reminders about upcoming events
- Good news regarding the school's performance, attainment or reputation
- Good news regarding the achievements of staff and pupils
- Information that parents should be aware of, e.g. school closure

Staff will ensure that their posts meet the following criteria:

- The post does not risk bringing the school into disrepute
- The post only expresses neutral opinions and does not include any personal views
- The post uses appropriate and school-friendly language
- The post is sensitive towards those who will read it, and uses particularly neutral and sensitive language when discussing something that may be controversial to some
- The post does not contain any wording or content that could be construed as offensive
- The post does not take a side in any political debate or express political opinions
- The post does not contain any illegal or unlawful content

Staff use of personal social media

All staff are expected to maintain the high standards of personal and professional conduct required by the Teachers' Standards and the Staff Code of Conduct, both in and outside school, including on personal social media accounts:

- staff must not contact current pupils, or accept contact from current pupils, via personal social media accounts or personal messaging apps. All communication with pupils takes place through school-approved channels;
- Staff must not keep in contact with past pupils until they are 18 or at least 3 years has passed since they left Appleford.
- staff are strongly encouraged to use the highest available privacy settings on personal accounts and to be mindful that content shared even on a “private” account may be screenshotted and shared further;
- staff must not post or share any confidential, personal or safeguarding information relating to pupils, parents or colleagues, or any photograph or video of a pupil, on a personal social media account;
- staff must not post content that could bring the school or the teaching profession into disrepute, that is discriminatory, derogatory about colleagues, pupils, parents or the school, or that could reasonably be perceived as such, even where the school is not named;
- any concern, complaint or disagreement about a school matter should be raised through the appropriate internal channel (e.g. line manager, Headmaster, Advisory body, proprietor or whistleblowing procedure where relevant) and not aired on social media;
- staff should exercise particular caution when discussing their profession online (for example in professional networking or forum posts), ensuring that no pupil, parent or colleague is identifiable, even indirectly, without consent and
- where a member of staff becomes aware of a concern about their own or a colleague's social media conduct, or about any contact between a member of staff and a pupil via social media, this should be reported promptly to the Headmaster or DSL in accordance with the school's procedures for managing allegations against staff and “low-level concerns” under KCSIE.

Staff will not be prohibited from having personal social media accounts; however, it is important that staff protect their professional reputation by ensuring they use personal social media accounts in an appropriate manner.

Staff will be required to adhere to the following guidelines when using personal social media accounts:

- Staff members will not access personal social media platforms during school hours.
- Staff members will not use any school-owned mobile devices to access personal accounts.
- Staff will not ‘friend’, ‘follow’ or otherwise contact pupils through their personal social media accounts. If pupils attempt to ‘friend’ or ‘follow’ a staff member, they will report this to the DSL or headmaster
- Staff will be strongly advised to not ‘friend’ or ‘follow’ parents on their personal accounts.
- Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school on their personal social media accounts.
- Staff will ensure it is clear that views posted on personal accounts are personal and are not those of the school.
- Staff will not post any content online that is damaging to the school, its staff or pupils.
- Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Staff will not post comments about the school, pupils, parents, staff or other members of the school community.

Safer Recruitment: Online Checks: In line with KCSIE 2026, as part of safer recruitment due diligence, the school carries out an appropriate online search of shortlisted candidates for posts at the school, to help identify any incidents or issues that have happened, and are publicly available online, that the school might want to explore with the applicant at interview. This is carried out proportionately, with regard to data protection principles, and any findings are discussed with the candidate as part of the recruitment process.

Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

Parent use of social media

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members, in accordance with the Social Media Code of Conduct for Parents.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the headmaster, and may have their ability to interact with the social media websites removed.

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

Pupil use of social media

EYFS to Key Stage 2

Most social media platforms set a minimum age requirement of 13 in their terms of service. Appleford does not provide younger pupils with personal social media accounts and does not expect them to use social media independently in connection with school activities.

- Where any school-managed online platform has a social or sharing element (for example, a closed class learning platform with a comment feature), this is used only under direct staff supervision and within a closed, school-controlled environment.
- Age-appropriate digital citizenship education helps pupils begin to understand that information shared online can be seen by others, and lays foundations for safe and responsible use of technology as pupils get older.

Key Stage 3 and Key Stage 4

Many pupils at Key Stage 3 and 4 will hold personal social media accounts outside school. The school does not control pupils' personal accounts, but expects the following standards of conduct in respect of anything connected with the school community:

- pupils must not use social media to bully, harass, threaten or be disrespectful towards other pupils, staff, or the wider school community, whether during the school day or otherwise;
- pupils must not post photographs, videos or personal information about other pupils or staff without their consent;
- pupils should not accept or send friend/follow requests to or from members of staff on personal accounts; any such request should be reported to a trusted adult;
- personal mobile phones and devices are not used to access social media during lesson time, in line with the Mobile Phone Policy; and
- pupils are taught, through the curriculum, about online reputation, digital footprint, the risks of sharing personal images, the warning signs of grooming or exploitation, and how to recognise and report extremist or radicalising content encountered online, in line with the Prevent duty.

Cyberbullying and Conduct Affecting the School Community: Where conduct on social media, even if it takes place outside school hours or off the school site, has an impact on relationships, safety or wellbeing within the school community (for example, cyberbullying between pupils, or content that disrupts good order and discipline), the school may address this under its Behaviour Policy and Anti-Bullying Policy. Any pupil affected by cyberbullying or other harmful conduct on social media is encouraged to report it to a trusted member of staff, who will follow the school's safeguarding and anti-bullying procedures.

Cyberbullying:

Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.

Guidance for Parents and Carers:

Appleford asks parents and carers to support a safe and respectful online environment for our whole school community:

- please do not post photographs or videos of pupils other than your own child on social media, including images taken at school events, without the consent of the other pupils' parents/carers;
- please raise any concern or complaint about the school, a member of staff, or another family directly with the school through the Complaints Policy, rather than on social media;
- please be aware that harassment, abuse or threatening behaviour directed at staff, pupils or other parents online may have legal consequences and will be taken seriously by the school;

- if your child is below the minimum age for a particular social media or messaging platform, the school recommends that they should not use it; the school is happy to share further guidance and resources on age-appropriate technology use on request; and
- for parents of older pupils, please remain engaged with your child's social media use where appropriate to their age, and contact the school promptly if you become aware of cyberbullying, harassment, or other harmful conduct connected with the school community, so that it can be addressed under the relevant policy.

Photography, Video and Image Consent:

- the school obtains and records parental consent before using a pupil's photograph or video for any marketing, communications or social media purpose, in line with the Data Protection Policy;
- consent preferences are reviewed periodically and can be withdrawn or amended by parents/carers at any time by contacting the school office; the school maintains an up-to-date record of consent preferences that is checked before any image is used;
- pupils are not named in a way that identifies them alongside their photograph on social media unless specific consent for this has been given and
- parents/carers attending school events are asked to respect the school's photography guidelines, including any restrictions on photographing or filming pupils other than their own child.

Monitoring, Compliance and Breaches of this Policy:

The Marketing/Communications Lead monitors official school social media accounts for comments or content requiring a response or escalation. The school does not routinely monitor staff personal social media accounts, but will investigate where a specific concern is raised in line with its disciplinary and safeguarding procedures.

Breaches of this policy by staff may be addressed through the school's disciplinary procedures and, in serious cases, may constitute gross misconduct or be referred to external bodies as required by law or regulation.

Pupils will not access social media during lesson time, unless it is part of a curriculum activity. Pupils will not be permitted to use the school's WiFi network to access any social media platforms unless prior permission has been sought from the headmaster, and an ICT technician has ensured appropriate network security measures are applied.

Pupils will not spread misinformation on social media, whether sharing posts or creating their own. Pupils will be mindful that AI tools available on social media may provide non-factual or misleading information. Pupils' use of AI is compliant with the Safe Use of AI Policy

Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Where a pupil attempts to 'friend' or 'follow' a staff member on their personal account, it will be reported to the DSL or headmaster. Pupils will not post any content online which is damaging to the school or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.

Pupils will be instructed not to sign up to any social media platforms that have an age restriction above the pupil's age or use an adult's ID to bypass safety measures to access social media platforms with age restrictions.

If inappropriate content is accessed online on school premises, this will be reported to a member of staff.

Breaches of this policy will be taken seriously and managed in line with the Behaviour Policy.

Data protection principles

The school will obtain consent from pupils and parents [at the beginning of each academic year](#) using the Social media consent form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the [entire academic year](#). Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

Where a pupil is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the pupil.

A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The DPO will be responsible for ensuring this consent record remains up-to-date.

Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing. Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and pupils' requirements following this. Wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.

Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided. The school will only post images and videos of pupils for whom consent has been received.

Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the online safety officer / DSL for use. Only appropriate images and videos of pupils will be posted in which they are suitably dressed, e.g. it would not be suitable to display an image of a pupil in swimwear.

When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.

When posting images and videos of pupils, the school will apply data minimisation techniques, such as anonymisation (blurring a photograph), to reduce the risk of a pupil being identified. The school will not post pupils' personal details on social media platforms and pupils' full names will never be used alongside any videos or images in which they are present.

Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

Any breaches of the data protection principles will be handled in accordance with the school's Cyber-security Policy.

Safeguarding considerations:

Social media raises specific safeguarding considerations for the school community:

- any contact between a member of staff and a pupil via personal social media or messaging apps is treated as a serious matter and managed in accordance with the school's procedures for managing allegations against staff;
- the use of any technology, including social media or image-editing tools, to create, share or request a sexualised or otherwise harmful image of a child or adult is strictly prohibited, will be treated as a serious child protection matter under the Safeguarding and Child Protection Policy, and may constitute a criminal offence; any concern of this nature must be reported to the DSL immediately; and
- any other safeguarding concern arising from social media use is reported and handled in accordance with the Safeguarding and Child Protection Policy.

Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour will be reported to the headmaster and DSL, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headmaster teacher, it will be reported to the proprietor.

Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the headmaster and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headmaster will contact the police. The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents what systems the school uses to filter and monitor online use. The school will also make it clear to parents what their children are being asked to do online for school, including what platforms, they will be asked to access and who from the school, if anyone, they will be interacting with online.

Blocked content

In accordance with the school's Cyber-security Policy, the online safety officer / DSL will ensure installation of firewalls on the school's network to prevent access to certain websites. The following social media websites are not accessible on the school's network:

- [X](#)
- [Facebook](#)
- [Instagram](#)

Exemptions to this block will be made for authorised staff for the sole purpose of managing the school's official social media accounts.

ICT technicians retain the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

Inappropriate content accessed on the school's computers will be reported to an ICT technician so that the site can be blocked. Requests may be made to access erroneously blocked content by submitting a blocked content access form to an ICT technician, which will be approved by the headmaster and DSL

Training:

- staff receive guidance on this policy and on professional conduct online as part of induction and ongoing safeguarding training;
- The proprietor will receive periodic briefings on the school's social media activity and any related incidents;
- age-appropriate digital citizenship education is built into the curriculum across all key stages, from foundational online safety awareness in EYFS to Key Stage 2, through to digital footprint, online reputation, cyberbullying and extremism-awareness content for Key Stage 3 and 4 pupils and
- parents/carers are provided with guidance on supporting safe and respectful use of social media in connection with the school.

Policy Review: This policy will be reviewed annually by the Headmaster and DSL, and approved by the Governing Body, or sooner in response to a significant incident or a change in relevant legislation or statutory guidance.

The school recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, staff will receive training in identifying potentially at-risk pupils. Staff will receive training on social media as part of their new starter induction. Staff will receive ongoing training as part of their development.

Pupils will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links. Pupils will be provided with material to reinforce their knowledge.

Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources, such as our Social Media Code of Conduct for Parents.

Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

Use of social media on behalf of the school must be approved by the headmaster prior to setting up sites. Please complete this form and return it to the headmaster.

Team details		
Department		
Moderator of site		
Purpose of using social media		
Please describe why you want to set up this site and the content of the site		
What are your aims and what do you hope to achieve by setting up this site?		
What is the proposed content of the site?		
Proposed audience of the site		
☐ Pupils of the school Ages: age range	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: name of school	☐ Members of the public
☐ Other (please give details)		
Proposed contributors to the site		
☐ Pupils of the school Ages: age range	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: name of school	☐ Members of the public
☐ Other (please give details)		
Administration of the site		
Names of administrators (the site must have at least two approved administrators)		
Who will vet external contributors? (Please state name and job role)		
Who will host the site?		
Proposed date of going live		
How do you propose to advertise for contributors?		
If contributors include pupils, how do you propose to inform and obtain the consent of parents or responsible adults?		
What security measures will you take to prevent unwanted or		

unsuitable individuals from contributing or becoming 'friends' and 'followers' etc. of the site?		
Approval		
Approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher.		
Marketing officer I approve the aims and content of the proposed site and the use of the school brand and logo.	Name	
	Signature	
	Date	
Headmaster I approve the aims and content of the proposed site and the use of the school brand and logo.	Name	
	Signature	
	Date	

Social media consent form

This consent form provides information pertaining to how Appleford School wishes to use personal data on social media, details the terms under which the school will use this data and requests consent for the school to use your personal data on social media.

Name of parent	
Name of pupil	
Year group	

Why do we need your consent?

The school requests the consent of parents on an [annual](#) basis to use images and videos of their child for a variety of different purposes.

Without your consent, the school will not use images, videos, names or other forms of personal data of your child on social media. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why will we be using personal data on social media?

The school wants to use certain types of data on social media to promote the positive and inclusive ethos of the school – we aim to celebrate our pupils' and school's achievements and social media allows us to do this.

Where the school uses images of individual pupils, the name of the pupil will not be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil will not be used to accompany the text.

If, for example, a pupil has won an award and their parent would like their name to be published alongside their image, separate consent will be obtained prior to this.

With your consent, the school may use personal data on social media, the school website, in school prospectuses and other printed publications, such as a newsletter.

Who will be able to see the data once it's on social media?

The school's privacy settings only allow people who have been accepted to view the content on our social media platforms; additionally, where it is possible, the school's settings do not allow for further sharing. Please note, this sharing restriction may not be possible on all social media platforms, meaning that, if the content has been posted and is subsequently shared, more people will be able to view that piece of content.

What are the conditions of use?

- This consent form is valid for [the current academic year](#).
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video on social media.
- The school will not include personal emails, postal addresses, or telephone or fax numbers on images or videos on social media.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may post pictures of work created by pupils on social media.
- The school may use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- The school will not post any sensitive data, such as details of SEND, without express and additional consent, and will then still anonymise the posts.

Providing your consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

The school will only post personal data on social media for the conditions that you provide consent for.

I provide consent to	Yes	No
Using images of my child on the school's social media accounts.		
Using videos of my child on the school's social media accounts.		
Using images of my child on social media, including the following: • Facebook • Instagram		
Using videos of my child on social media, including the following: • Facebook • Instagram		
Using my child's first name on social media.		
Using my child's age on social media.		

Refreshing your consent

This form is valid for [the entire academic year](#), it will be updated on an [annual](#) basis. Parents are required to fill in a new form for their child [every academic year](#).

Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the data protection officer (DPO). A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing personal data that was shared prior to withdrawal; however, the school will make every effort to remove posts about the pupil where possible, e.g. images of the pupil on social media will be removed.

If you would like to withdraw your consent, you must submit your request in writing to the DPO.

Declaration

I, _____ (name of parent), understand:

- Why my consent is required.
- The reasons why Appleford School uses my child's personal data on social media.
- Who will be able to view my child's personal data once posted.
- The conditions under which the school uses personal data of my child on social media.
- I have provided my consent above as appropriate, and the school will act in accordance with my requirements.
- Consent is refreshed on an [annual](#) basis and I must re-provide consent in subsequent academic years.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the DPO.

Name of parent:

Signature:

Date:

If you have any questions regarding this form, please do not hesitate to contact the DPO at secretary@appleford.wilts.sch.uk

Appendix A: Staff Quick Reference

Do:

- Keep personal and professional social media use clearly separated.
- Use the highest available privacy settings on personal accounts.
- Report any contact from a pupil via personal social media to the DSL immediately.
- Raise concerns about the school through internal channels, not online.

Do not:

- Contact pupils, or accept contact from pupils, via personal social media or messaging apps.
- Post photographs, videos or personal information about pupils, parents or colleagues without authorisation.
- Post content that could bring the school or the profession into disrepute.
- Post on an official school account without authorisation.

Appendix B: Glossary

Term	Meaning
Social Media	Websites and applications that enable users to create and share content or to participate in social networking, including messaging apps with public or semi-public features.
Official Account	A social media account created and managed by the school for school purposes, as opposed to a personal account belonging to a staff member, pupil or parent.
Low-Level Concern	A concern, under KCSIE, about behaviour by a member of staff that does not meet the threshold of a safeguarding allegation but which should nonetheless be recorded and addressed.
DSL	Designated Safeguarding Lead – the senior member of staff with lead responsibility for safeguarding.
DPO	Data Protection Officer – the person responsible for advising the school on data protection compliance.
Prevent Duty	The statutory duty on schools to have due regard to preventing people being drawn into terrorism, including online radicalisation.
Cyberbullying	Bullying that takes place using electronic means, such as social media, messaging apps, or online gaming platforms.
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]
[Insert]	[Insert]

Appendix C: Official Social Media Accounts Register

This register is maintained by the Marketing/Communications Lead and reviewed at least annually.

Platform	Account Name/Handle	Administrator(s)	Approved By / Date
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]
[Insert]	[Insert]	[Insert]	[Insert]