

St. John's C of E (VA) Primary School Social Media Policy



‘That all may Love, Learn, Flourish’

Date:	Autumn 2025
Frequency of review	1 year
Reviewed by	Personnel

Owner (job role):	DSL/DHT
Approval Body:	Personnel
Approval Date:	Autumn 2025
Implementation Date:	Initial implementation date: New implementation date:
Next Review Date:	

Version	Approval date	Summary of changes
1		New policy using template from National College (formerly School Bus) to ensure compliance with updated legal framework and latest DfE guidance.

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. School social media accounts
4. Staff use of personal social media
5. Parent social media use
6. Pupil use of social media
7. Data protection principles
8. Safeguarding
9. Blocked content
10. Cyberbullying
11. Training

Appendices

- a) KS1 Pupil Acceptable Use Agreement
- b) KS2 Pupil Acceptable Use Agreement

Statement of intent

At St. John's, our vision ('That all may Love, Learn, Flourish') underpins all that we do. St. John's understands that social media is a growing part of life outside of school and we welcome responsible participation by members of the school community in a way that enables children to flourish. 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 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 cyber bullying and potentially career-damaging behaviour.
- Informing parents/carers of the importance of online safety.

1. Legal framework

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

- DfE 'Data protection in schools'
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- DfE 'Keeping children safe in education 2025'
- Online Safety Act 2023

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement for Staff
- Acceptable Use Agreement for Pupils
- Online Safety Policy
- Data Protection Policy
- Complaints Policy and Procedures
- Anti-bullying Policy
- Child-on-child Abuse Policy
- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- Disciplinary Policy and Procedure
- Behaviour Policy

2. Roles and responsibilities

The governing board will be responsible for:

- 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 headteacher will be responsible for:

- 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 governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the number of misplaced or malicious allegations in relation to social media use.
- Working alongside the DPO and ICT technicians to ensure appropriate security measures are implemented and compliance with UK GDPR and other data protection legislation.

The DSL will be responsible for:

- The school's approach to online safety.
- Dealing with concerns about social media use that are safeguarding concerns.

Staff members will be responsible for:

- Adhering to the principles outlined in this policy and the Acceptable Use Agreement for Staff.
- 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 headteacher immediately.
- Attending any training on social media use offered by the school.

Parents will be responsible for:

- Adhering to the principles outlined in this policy.
- 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.
- Attending meetings held by the school regarding social media use wherever possible.

Pupils will be responsible for:

- Adhering to the principles outlined in this policy and the relevant Acceptable Use Agreement.
- 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.
- Demonstrating the same high standards of behaviour as expected within the school.

ICT technicians (Cygnet) will be responsible for:

- Providing technical support in the development and implementation of any school social media accounts.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

3. School social media accounts

At the current time, St. John's does not have any school social media accounts.

Social media accounts for the school will only be created by the marketing officer and other designated staff members, following approval from the headteacher. 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 headteacher 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 headteacher 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 headteacher.

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 the marketing officer will post on school social media accounts.

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

4. Staff use of personal social media

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:

- In line with our Use of Mobile Devices Policy, staff members will only use personal mobile devices in areas not accessed by pupils during designated break times, e.g. the staff room.
- Staff members will not use any school-owned 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 headteacher.
- 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.

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.

5. Parent use of social media

At the current time, St. John's does not have any school social media accounts.

Parents may be able to comment on or respond to information shared via school 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.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the headteacher, 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.

6. Pupil use of social media

Pupils do not have access to mobile devices during the school day.

Pupils will adhere to the relevant KS1/KS2 Acceptable Use Policy (see Appendices).

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 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 headteacher.

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.

7. Data protection principles

If the school were to create a social media account, the school would obtain consent from parents to confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. 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.

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 would be able to withdraw or amend their consent at any time. To do so, parents must inform the school in writing. Where parents 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.

Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the 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' or 'netball team.'

When posting images and videos of pupils, the school will apply data minimisation techniques, such as pseudonymisation (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 Data Protection Policy.

8. Safeguarding

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 headteacher, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct and Disciplinary Policy and Procedures. If the concern is about the headteacher, it will be reported to the chair of governors.

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 headteacher 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 headteacher 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.

9. Blocked content

The ICT technicians will install 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
- LinkedIn

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 headteacher.

10. 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.

11. Training

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 development.

Pupils will be educated about online safety and appropriate social media use on a regular basis through a variety of mediums, including unplugged computing lessons, PSHE/RHE lessons and collective worships.



Parents will be sent a regular Online Safety Newsletter, back copies of which will be available on the school website.

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



Acceptable Use Policy (AUP) for KS1 PUPILS

My name is _____

1. I only **USE** devices or apps, sites or games if I am allowed to.
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused.
3. I look out for my **FRIENDS** and tell someone if they need help.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE**. [to mention AI might be too much for KS1 but insert here if you are going to talk about examples]
6. Anything I do online can be shared and might stay online **FOREVER**.
7. I don't keep **SECRETS**  unless they are a present or nice surprise.
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must.
9. I don't change **CLOTHES** or get undressed in front of a camera. I don't wear my underwear or swimwear in front of a camera.
10. I always check before **SHARING** my personal information or other people's stories, videos and photos.
11. I am **KIND** and polite to everyone.

My trusted adults are:

_____ at school
_____ at home
_____ at _____ [other places]

children may spend time e.g. a place of worship, childminder, Rainbows, etc.]



These statements can keep me and others safe & happy at school and home

- I learn online** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
- I behave the same way on devices as face to face in the classroom, and so do my teachers** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
- I ask permission** – At home or school, I only use devices, apps, sites and games if and when I am allowed to. If not sure, I will ask.
- I am creative online** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
- I am a good friend online** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them!
- I am not a bully** – I know just calling something fun or banter doesn't stop it may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos and if I see it happening, I will tell my trusted adults.
- I am a secure online learner** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
- I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
- I know it's not my fault if I see or someone sends me something bad** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
- If I make a mistake I don't try to hide it but ask for help.**
- I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about.
- I know online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
- I never pretend to be someone else online** – it can be upsetting or even dangerous.
- I check with a parent/carer before I meet an online friend** the first time; I never go alone. I will not plan to meet anyone I have communicated with online unless I am with a trusted adult.
- I don't go live (videos anyone can see) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.



- I don't take photos or videos or people without them knowing or agreeing to it** – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
- I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with a camera. I don't wear underwear or swimwear while on camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
- I can say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
- I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
- I follow age rules** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
- I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
- I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
- I am a rule-follower online** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
- I am part of a community** – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it.
- I respect people's work** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
- I am a researcher online** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.
- I do not use AI tools to complete school work or homework.** This includes ChatGPT (which has an age limit of 13+).
I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school that might mean _____
Outside school, my trusted adults are _____

Name: _____ Signed: _____

Date: _____