Woodstock CE Primary

Hand in hand we...
Love | Learn | Flourish

Policy for:

Social Media

		Date
Reviewed by:	SLT	Dec 2024
Authorised by:	H&S	Spring 2025
Date for next review: (or earlier should legislation require it)	Spring 2026	

Woodstock CE Primary

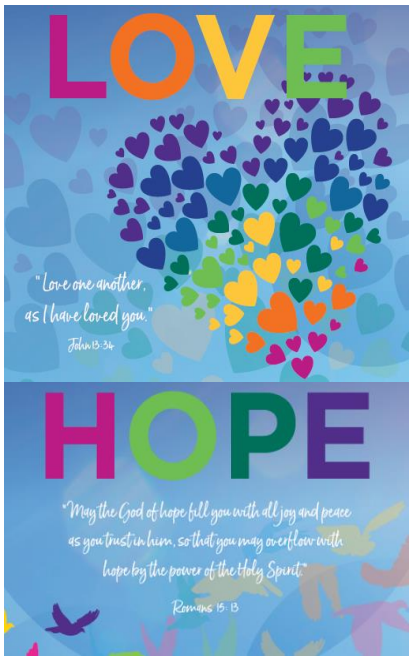
Hand in hand we…
Love | Learn | Flourish

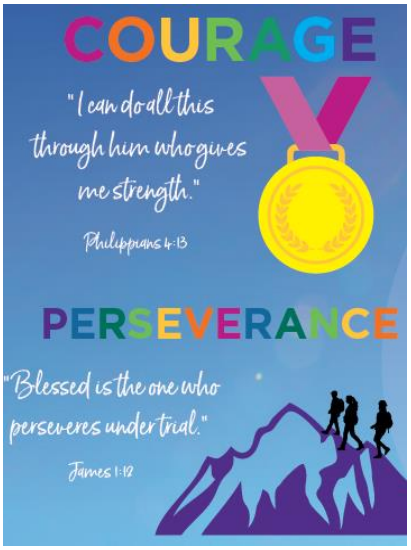
Our Christian Vision & Values

Our Christian vision states that we:
Clear a path for a lifelong journey of exploration and growth, through an innovative and challenging curriculum, inspiring all in our community to be courageous advocates and global citizens. Everyone can find their light and shine it brightly. Hand in hand, we love, learn and flourish together.

'In the same way, let your light shine before others, so that they may see your good works and give glory to your Father who is in heaven.' 'Let your light shine' Matthew 5:16

Our core Christian values allow us to deliver the Christian vision:





Social Media Policy

Statement of Intent

Woodstock CE Primary School understands that social media is a growing part of life outside of school. 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 Christian vision, 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.
- Updating parents/carers about issues relating to online safety e.g. National Online Safety Wake Up Wednesday parent guides.

Legal Framework

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

- DfE (2023) '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' (latest version, including updates)

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement for Pupils
- Acceptable Use Agreement for Staff
- Staff and Volunteer Handbook
- Online Safety Policy
- Data Protection Policy
- Complaints Procedures Policy
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- School Social Media Accounts – Terms of Use Agreement.
- Staff Code of Conduct
- Confidentiality Policy
- Child Protection and Safeguarding Policy
- Disciplinary Policy and Procedure
- Behaviour Policy

Roles and Responsibilities

The governing board is 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 is 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 amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the DPO and Network Manager to ensure appropriate security measures are implemented and compliance with UK GDPR and other data protection legislation.

The DDSL/Online Safety Lead is responsible for:

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

Staff members are 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 are responsible for:

- 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 them and their children.
- Attending meetings held by the school regarding social media use wherever possible.

Pupils are responsible for:

- 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.
- Demonstrating the same high standards of behaviour as expected within the school.

The Network Manager and School Business Manager is responsible for:

- 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.
- Ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.
- 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.

Network Manager (123ICT) 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 headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

School Social Media Accounts

Social media accounts for the school will only be created by the School Business Manager and other designated staff members (SLT), 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 has been 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 by the School Business Manager.

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 School Business Manager 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 School Business Manager or another designated member of staff.

Staff Conduct

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

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

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 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 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.

Parent Social Media Use

Parents can 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 Acceptable Use Policy for Parents.

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.

Pupil Social Media Use

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 headteacher, and the Network Manager has ensured appropriate network security measures are applied.

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 are instructed not to sign up to any social media platforms that have an age restriction above the pupil's age. 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 parents using the schools consent form, which will confirm whether consent is given for posting images and videos of a pupil on social media platforms. Consent provided for the use of images and videos 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 via ParentMail, which details the pupils for whom consent has been provided.

Parents can 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' 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 from 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 School Business Manager 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 without consent, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified, or child will not be photographed at all. 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 ParentMail records 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 Online Safety Policy.

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, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it will be reported to the chair of governors. LADO involvement will be sought if required.

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 Network Manager, 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 because of ignorance or normal developmental curiosity. 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. Referral to MASH will be made as appropriate.

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 & Filtering Systems

In accordance with the school's Online Safety Policy, the School Business Manager with support from our Network Lead (123ICT) will install firewalls and secure filtering systems on the school's network to prevent access to certain websites. Social media websites are not accessible on the school's network at all.

The School Business Manager with support from our Network Lead (123ICT) retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices through our robust filtering system which provides immediate alerts.

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 the School Business Manager so that the site can be blocked. Requests may be made to access erroneously blocked content by submitting a blocked content access form to the School Business Manager, which will be approved by the headteacher.

Cyberbullying

Cyberbullying is making use of information and communications technology, particularly mobile phones and the internet, to deliberately undermine, humiliate or otherwise cause distress to the person on the receiving end. Staff must not use social media and the internet to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations (including Woodstock CE Primary School).

Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

It should be noted that a person does not need to directly experience this form of victimisation for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

Staff do not personally engage with cyberbullying incidents and should immediately report incidents to the Head Teacher or Online Safety Lead (DSLs). If a member of Staff is the victim (receives any threats, abuse, or harassment from members of the public through their use of social media), they should keep any records of the abuse and if appropriate, screen prints of messages or webpages with time, date and address of the site. Staff must report such incidents using the school's procedures. Support is also available through confidential counselling support.

The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/pupils or parents, whether this takes place during or outside of work.

Staff members and pupils need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, other pupils, or parents, can find its way into the public domain even when not intended. 64. If a member of staff is the perpetrator of the incident/s the situation will then be investigated and if appropriate, the Disciplinary or Capability Procedure will be followed.

If a pupil is the perpetrator of the incident/s the situation will be initially investigated in line with the school behaviour and pupil disciplinary policy. Where appropriate the police will be consulted. Where a potential criminal offence has

been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police enquires. Staff who are victims of cyber-bullying or harassment will be offered support by their line manager and where suitable, occupational health.

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.

Senior Leadership Responsibility in Relation to Online Bullying and Harassment

The school owes a duty of care to our staff to take reasonable steps to provide a safe working environment free from bullying and harassment. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, X, or by any other means.

If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

Senior Leaders encourage staff to preserve all evidence by not deleting emails. In addition, logging phone calls and taking screen-prints of websites would all help towards supporting an investigation. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team will consider advising the employee that they should inform the police.

If such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police will be contacted immediately for advice.

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 ongoing training as part of their development. New staff will receive cyber training as part of their induction.

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

Training for all pupils and staff will be refreshed considering any significant incidents or changes – this includes changes to Keeping Children Safe in Education, Prevent, and Government Policy etc.

Monitoring and Review

This policy will be reviewed on an annual basis by the headteacher and governing board.

The next scheduled review date for this policy February 2026