

# Juniper Hill School

## **Social Media Policy**



*Kindness    Enjoyment    Achievement*

Written January 2024  
Reviewed January 2026

Next review January 2028

## **Contents:**

### Statement of intent

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

### **Appendices**

- A. Blocked content access request form
- B. Inappropriate content report form

## Statement of intent








Juniper Hill 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 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.
- 🏠 Providing online safety information for our families

## 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 (2023) 'Keeping children safe in education 2023'

This policy operates in conjunction with the following school policies:

-  Use of images / videos for Parents
-  Acceptable Use Agreement for Staff
-  Acceptable Use Agreement for Pupils
-  Online Safety Policy
-  Data Protection Policy
-  Pupils Code of Conduct
-  Complaints Procedures Policy
-  Anti-bullying Policy
-  Allegations of Abuse Against Staff Policy
-  Low-level Safeguarding Concerns Policy
-  Photography and Images Policy
-  Staff Code of Conduct
-  Confidentiality Policy
-  Cyber-security Policy
-  Child Protection and Safeguarding Policy
-  Disciplinary Policy and Procedure
-  Behaviour Policy

## 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 body, 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 IT Manager 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 meeting held by the school / reading the resources shared in the newsletter regarding social media use wherever possible.

Pupils will be 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.










IT Manager will be responsible for:

-  Implementing appropriate security measures as directed by the headteacher.
-  Ensuring that the school's filtering and monitoring systems are updated as appropriate.

### **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 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.

### **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 IT 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 pupils and parents at the beginning of each key stage using the photograph and video consent form, which will confirm whether or not consent is given for posting images and videos of a pupil in the newsletter / on the school website. The consent will be valid for the entire key stage. Consent provided for the use of images and videos only applies to school – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

A record of consent is maintained, 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 are 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' 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 the school website.



Consent can be provided for certain principles only, for example only images of a pupil are permitted to be shared, 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 for use. Only appropriate images and videos of pupils will be shared in which they are suitably dressed, e.g. it would not be suitable to display an image of a pupil in swimwear.

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

When sharing 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 sharing images / videos, 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**

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.




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 IT 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 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 IT Manager / Turn IT On 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

The IT Manager retains 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 IT 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 IT Manager, which will be approved by the headteacher.

### **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.

### **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 online safety as part of their new starter induction. Staff will receive regular and ongoing training 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 assemblies, PSHE lessons, Life Skills lesson 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 periodically and provided with online safety information in the weekly newsletter.

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

**Monitoring and review**

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

Any changes made to this policy will be communicated to all staff, pupils and parents.

## Appendix A - Blocked content access request form

<b>Requester</b>	
<b>Staff name</b>	
<b>Date</b>	
<b>Full URL</b>	
<b>Site content</b>	
<b>Reasons for access</b>	
<b>Identified risks and control measures</b>	
<b>Authoriser</b>	
<b>Approved?</b>	
<b>Reasons</b>	
<b>Staff name</b>	
<b>Date</b>	
<b>Signature</b>	

**Appendix B - content report form**

<b>Staff name (submitting report)</b>	
<b>Name of individual accessing inappropriate content (if known)</b>	
<b>Date</b>	
<b>Full URL(s)</b>	
<b>Nature of inappropriate content</b>	
<b>To be completed by IT Manager</b>	
<b>Action taken</b>	
<b>Staff name</b>	
<b>Date</b>	
<b>Signature</b>	