



Acceptable Use Policy

Reviewed: September 2026

Next Review: September 2027

Approved by: the Board of Governors

What is an AUP?

We ask all children, young people and adults involved in the life of our school to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers will be asked to sign it when they join or are appointed and whenever significant changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal and professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the Social Media Policy.

Where can I find out more?

All staff, governors and volunteers should read the school's Online Safety Policy and Social Media Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy).

If you have any questions about this AUP or our approach to online safety, please speak to the Executive Headteacher or Head of School.

What am I agreeing to?

I have read and understood the school's Online Safety Policy and Social Media Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Head of School or Executive Headteacher (if by an adult).

I will follow the guidance in the school's Online Safety Policy, Social Media Policy and Safeguarding and Child Protection Policy for reporting incidents. I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sharing nudes and semi-nudes, including digitally altered or AI-generated sexual imagery, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

I will take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter (this includes bullying, sexual violence and harassment) and maintain an attitude of 'it could happen here'.

I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

I understand the responsibilities listed for my role in the school's Online Safety Policy and Social Media Policy. This includes promoting online safety as part of a whole school approach in line with the PSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

Remote learning

The same professional standards and safeguarding expectations apply during remote learning as they do in school. Any online lesson, meeting or tutoring session involving a pupil must have the prior approval of the school and must take place through an approved, school-managed system. Personal accounts, devices or login details must not be used to communicate privately with pupils or deliver remote teaching unless this has been expressly authorised by the Executive Headteacher or Head of School.

Remote lessons must be conducted in a professional environment. Staff should dress appropriately, ensure that the camera does not display personal information or unsuitable objects, and use a virtual or blurred background where necessary. Recordings or screenshots of pupils or staff must not be taken unless this has been approved for a clear educational purpose. Any inappropriate incident or safeguarding concern arising during a live lesson must be reported immediately to the Designated Safeguarding Lead where it relates to a child, or to the Head of School or Executive Headteacher where it relates to an adult. Staff must remain particularly alert to the increased risks of grooming and exploitation during periods when pupils are spending more time at home and online.

School systems and monitoring

School systems, accounts and devices are provided for professional use and remain the property of the school. Their use may be monitored through SENSO and other automated or manual systems, including the monitoring of files, activity and content. Where there is a legitimate reason to do so, appropriately authorised staff may access school accounts or information held on school systems. SENSO monitoring and the school's filtering arrangements may also apply when school accounts or systems are accessed from a personal device or away from the school site, regardless of the time, location or connection used.

Online communication and professional conduct

All users are expected to model safe, responsible and respectful online behaviour. Images or personal information relating to others must not be shared or published without permission, and negative, threatening, discriminatory or violent comments must not be posted. Contact with pupils must only take place through school-approved and school-monitored channels. Any attempt by a pupil or another person to make contact outside these arrangements must be reported to the Head of School. Expectations relating to social media, digital images, video and personal devices are set out in the Social Media Policy, and advice must be sought from the Head of School whenever there is uncertainty about whether an action is permitted.

Data protection and account security

School information must be handled in accordance with the Data Protection Policy. Users must only access, store or share information where they have permission to do so and must not store school-related data on personal devices, personal cloud storage or other unapproved platforms. Personal data sent by email must be protected appropriately, including using Egress or password protection where required, with passwords communicated separately. Anything written about an identifiable person may be disclosed through a Subject Access Request and must therefore remain factual, professional and consistent with the Staff Code of Conduct.

Passwords and login details must be strong, unique and kept confidential. Accounts must not be shared, and users are responsible for activity undertaken while they are logged in. Passwords must be changed immediately if there is any reason to believe they have been compromised, and devices must be locked

whenever they are left unattended. Suspicious emails must be reported before any links or attachments are opened or login details are entered. Suspicious emails should not be forwarded; a screenshot should be provided when reporting them. Care must also be taken when selecting email recipients, using CC or BCC, and attaching documents.

Acceptable use of technology

Only approved and appropriately licensed software, hardware, systems and online services may be used. School devices and networks must not be used to access illegal, extremist, offensive or otherwise inappropriate material, bypass security or monitoring arrangements, or support organisations or individuals whose activities are inconsistent with the school's values and legal responsibilities. Hardware or software must not be installed without permission from the IT Department, and all equipment loaned by the school must be kept secure and looked after properly.

Personal social media accounts must not be used for school business or presented as official school accounts. Where a member of staff can be identified as connected with the school, anything posted must remain professional and must not compromise safeguarding, confidentiality or the reputation of the school. All members of the school community are expected to uphold the commitments contained within the Acceptable Use Policy and report any suspected breach through the appropriate school procedures. A breach may result in disciplinary action, the withdrawal of access to school systems, the ending of a person's relationship with the school or, where appropriate, referral to the relevant authorities.

ACCEPTABLE USE AGREEMENT

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature	
Name	
Role	
Date	

To be completed by Head of School or Executive Headteacher

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems (T drive/P drive, etc.)	
Additional permissions (e.g. admin)	
Signature	
Name	
Role	
Date	



School Social Media Policy and Guidance

Reviewed: September 2026

Next Review: September 2027

Approved by: the Board of Governors

Introduction

The rationale of this policy is to set out clear expectations for the acceptable use of social media, including Bevington Primary School's official Instagram account. The policy applies to staff, pupils, parents, carers, governors, volunteers and any other individuals directly associated with the school, whether social media is used for school or personal purposes.

The purpose of using Instagram at Bevington is to:

- Communicate key messages with our school community, including reminders, alerts and updates.
- Celebrate achievements of pupils and staff, and share successes across the curriculum.
- Promote school events, trips, and wider opportunities.
- Strengthen links between school and home through regular communication.

This policy also ensures that the use of social media supports and aligns with the school's safeguarding, behaviour, equalities, and data protection policies. It applies whether social media is accessed on school equipment, personal devices, or other internet-enabled equipment, and whether during or outside of school hours.

Staff, pupils, parents and carers are expected to read and comply with this policy. Everyone must remember that content shared online, even in private spaces, may still be subject to safeguarding, copyright and data protection legislation.

For the purposes of this document, 'social media' refers to all online platforms and technologies that allow individuals to communicate and share information, photos or videos. This includes, but is not limited to, group messaging applications such as WhatsApp.

Instagram

Bevington Primary School uses its official Instagram account to share images, videos and updates with approved followers. The account supports communication of school news, celebrates achievements and provides timely information to parents and carers. It is managed by designated staff and is not used for private or direct messaging with users. The account is private and its content can only be viewed by followers approved by the school.

The primary purpose of the account

Bevington Primary School currently uses Instagram as its main social media platform to share the work of the school and promote the achievements of staff and pupils. Our official Instagram account is @bevingtonw10, and this is used to celebrate successes across the curriculum, highlight special events and provide an additional way of communicating with our community. The account is private so that the school can exercise greater control over who can view and interact with its content. The use of social media runs alongside more traditional communication methods, such as letters home, and is not intended to replace them. When using images of pupils, or groups of pupils, no names will be included. Where parents have indicated that they do not wish their child's image to be used on the school website or in public arenas, this preference will also be respected with regard to the school's social media accounts.

Controlling content for the account

The uploading of content to the school's Instagram account will be managed by designated staff at Bevington Primary School. All photographs and materials are to be sent to the Head of School for approval

before publication, and the Head of School has the final decision on what is shared. This ensures that all content is appropriate, consistent with school values, and compliant with safeguarding requirements.

Account followers

Requests to follow the school's private Instagram account are reviewed by designated staff. Access will only be approved where the account appears appropriate and the school is satisfied that granting access is consistent with safeguarding and the purpose of the page. The school may decline requests and remove or block followers at any time. The follower list is reviewed regularly, and parents and carers are reminded not to copy, download or reshare images or videos from the account without permission.

Interaction with other accounts

The school's social media presence is primarily used to share information. It will only follow accounts connected to education or with a clear educational purpose. Designated staff, under the direction of the Head of School, will remove abusive, discriminatory, offensive, spam or personally identifying content and may block users who repeatedly post inappropriate material. Serious concerns will be reported through the appropriate safeguarding, complaints or legal route.

Guidance for posting

Interactions from the school account, such as liking or resharing posts, will only take place where they are directly relevant to the school's purpose and consistent with this policy. All captions will be written in Standard English, avoiding text-speak, though hashtags may be used where appropriate to extend the reach of school communications. Staff are not permitted to use or link their personal social media accounts through the school's Instagram, nor should they follow the school account using their own personal profiles. Direct messaging through Instagram will not be used to communicate with external users, ensuring that all communication remains open and transparent.

Personal use of social media

Staff, governors and volunteers must not use personal accounts to conduct school business, communicate privately with pupils, share identifiable information or images relating to pupils, or publish content that could compromise safeguarding, confidentiality or the reputation of the school. Any safeguarding concern or contact received from a pupil through a personal account must be reported immediately to the Designated Safeguarding Lead.

Pupils, parents and carers

Concerns or complaints about the school must be raised through the school's official channels and dealt with under the Complaints Policy, rather than through social media. The same expectations of respectful communication apply in class WhatsApp groups and other private group-messaging services. Images of other people's children must not be posted without permission.

Digitally altered and AI-generated content

No member of the school community should create or share harmful, misleading, sexualised or non-consensual content relating to pupils, staff or others associated with the school, including deepfakes or other material altered or generated using artificial intelligence. Concerns will be addressed under the relevant safeguarding, behaviour, staff conduct or complaints procedures.

Artificial intelligence can make it easier to create convincing false images, audio, video and written content, impersonate real people and distribute harmful or misleading material quickly. The school will not assume that online content is genuine and will not dismiss a concern simply because material may have been generated or altered using AI. Concerns involving pupils or staff will be preserved as evidence, reported promptly to the Designated Safeguarding Lead or Head of School as appropriate, and managed through the relevant safeguarding, behaviour, staff conduct or complaints procedures.

The school supports pupils through age-appropriate teaching about consent, privacy, image sharing, deepfakes, impersonation, scams, misinformation and how to report worrying content. Staff are expected to remain alert to these risks and receive guidance on recognising and escalating concerns. Before AI-generated or digitally altered content is published through an official school account, designated staff will check its accuracy, suitability, copyright position and potential impact on safeguarding, privacy, bias and the school's reputation. Personal data relating to pupils or staff must not be entered into an AI tool unless its use has been expressly approved by the school and complies with data protection requirements.

Monitoring and review

The Head of School will monitor the implementation of this policy. It will be reviewed annually and approved by the Board of Governors.

Links with Other Policies

The following Bevington policies should be read in conjunction with this policy. All can be accessed from our website at: <https://www.bevington.rbkc.sch.uk/Policies/>

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- School Data Protection Policy
- Mobile Phones/Electronic Devices and Photography Policy
- Complaints Policy