Hindhayes Infant School

Acceptable Use Policy

September 2026

At Hindhayes, we believe success is based on the partnerships between pupils, staff and the parent community. We endeavour to enrich and develop each child to be a successful individual that will become an active community citizen of the future.

Approved on: _____

Signed: _____

Role: _____

Statutory requirements

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of key legislation and key definitions are:

• **online abuse** - Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2021; Welsh Assembly Government, 2018).

• **bullying** - Bullying is when individuals or groups seek to harm, intimidate or coerce someone who is perceived to be vulnerable (Oxford English Dictionary, 2021) It can involve people of any age, and can happen anywhere – at home, school or using online platforms and technologies (cyberbullying). This means it can happen at any time.

• **child protection** -The Department for Education (DfE) is responsible for child protection in England. It sets out policy, legislation and statutory guidance on how the child protection system should work. Somerset Safeguarding Children Partnership policy, procedure and guidance supports at a local level.

The Somerset County Council, Avon and Somerset Constabulary and Somerset Clinical Commissioning Group – now have joint and equal responsibility to safeguard children and young people, under the name of the Somerset Safeguarding Children Partnership. On the 20th May 2022 and updated on 1st September 2025, the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 1st September 2026

All education provisions have a responsibility to provide a safe and secure environment in which children can learn.

School Networks

(the school domain and wireless network)

- Staff must always keep their password private, must not share it with others, **unless authorised to do so,** and must not leave it where others can find it;
- Passwords should be at least 8 characters in length and include upper and lower case letters and also include numbers or symbols.
- Passwords are required to be changed frequently and users will be prompted to do this automatically.
- Computers that are left unattended must be either logged out or locked. Ctl + windows key+L
- The Wireless Network Key must not be shared with anyone. The office staff will manage this for any visitor to the school if required.

Email

- School emails must not be used for personal emails.
- Class teachers to use specific class emails
- Personal emails must not be used for school business.
- Staff email communications with pupils will only be carried out using Education email accounts. Staff are not to message or email pupils directly unless this is for a specific reason authorised by the Head Teacher: e.g. communication with EAL families.
- If a child tries to contact a member of staff via digital mediums then a member of the DSL will be informed
- Headteachers should not be routinely be copied in to emails to parents where the subject is at everyday classroom level. Should the email be more concerning then there should be a discussion with SLT and the Headteacher, Deputy Head or Parent Family Support Advisor may be copied in.

Mobile Devices (including Bring Your Own Device (BYOD))

- County email may be added to BYOD, e.g. tablets and mobile phones, but these devices must be password protected.
- Staff ipads are provided to staff for school use and must be password protected.
- Pupil devices (ipads & laptops) are not allowed to be removed from the school site. Unless agreed with the SLT for the purposes of remote learning
- Mobile phones will be either turned off / muted or locked away during lesson time, unless prior permission is sought from the SLT.
- Mobile phones will be stored in a prudent place during teaching time unless prior permission has been granted by SLT in extreme circumstances.
- Private phone calls can**not** be made during lesson time unless prior permission is sought from the SLT in extreme circumstances.
- BYOD must not be used to take photos or videos of the children or staff unless prior permission is granted.
- Regular monitoring and filtering reports will be completed by the Office Team and shared with the Headteacher to ensure these guidelines are being adhered too.

Social Networking (in school and private)

- Private social networking must not be used during lesson or directed times.
- Staff must not post anything about other members of staff, pupils, parents or the school in general, especially anything that brings the school into disrepute.
- Correct channels should be used to communicate school-based issues, this may be through staff whatsap groups to respond to urgent updates and messages.

Photos and Videos

- No photos or videos of pupils or staff will be taken without permission.
- No photos of pupils or staff will be taken on private devices unless prior permission is granted.
- Areas or No Filming Zones include toilets and any changing areas.

Concerns

- If any staff member or volunteer has a concern then the action taken would be to follow the procedures of the Low Level Concern Policy or the Whistle Blowing Policy.

Low Level Concerns Policy: https://www.hindhayes.co.uk/attachments/download.asp?file=2238&type=pdf
Whistle Blowing Policy: https://www.hindhayes.co.uk/attachments/download.asp?file=2178&type=pdf

All staff will read and agree this policy as a part of annual Safeguarding procedures.

Name_____ **Date**_____

Quick View Chart of acceptable use.

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selecte staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones/wearable technology in school		✓						✓
Use of mobile phones/wearable technology in lessons				✓				✓
Use of mobile phones/wearable technology in social time	✓							✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of personal devices including wearable technology				✓				✓
Use of 'always on' voice activated technology				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat facilities, forums and closed groups in apps		✓						✓
Use of messaging apps				✓				✓
Use of social networking sites including live broadcasting				✓				✓
Use of blogs e.g. when researching		✓						✓
Use of Twitter e.g. when networking		✓						✓
Use of video broadcasting e.g. YouTube		✓						✓