Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club

Acceptable Use Policy

Updated: September 2025
Review Date: September 2028

New technologies are now a big part of most people's lives, both in and out of school. The internet and other digital tools offer many new opportunities for learning and communication. They can help spark discussion, boost creativity, and support better learning for all. These tools also help teachers work more creatively and efficiently. It is vital to keep staff, governors, children and school visitors safe at Woodlands Primary School, Hedgehogs Nursery and Sunbeams Club (the school) as well as the schools IT systems and devices. This Acceptable Use Policy, when followed, will help to keep everyone safe as well as the schools IT systems and users protected from mistakes or misuse that could cause problems or security risks.

Scope

This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- email systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- computing devices – *this covers ANY computing device used for work purposes, whether at the place of work, home or elsewhere*
- photocopying, printing and reproduction equipment
- documents and publications (any type or format)

Acceptable Use Policy Agreement

The school is committed to providing staff and volunteers with good access to ICT to support their work both in and out of school, and to enhance pupils' learning. In return, the school expects all staff and volunteers to use ICT responsibly by agreeing to and following the guidelines outlined below.

Computer Security and data Protection

- Every staff member will get their own school computer account with a personal username and password. This account will match the level of access they need and should not be shared.
- Passwords must be strong. Use three random words with capital letters, numbers, and symbols. Never share your password with anyone and they should not be kept near or on any computing device.
- Passwords for any school device (computers, laptops, iPads, tablets etc) should not be given to children.
- Each laptop has a Bitcode for access. Staff must not store this Bitcode on or near their laptops
- Children should not use staff accounts. If they do (which is not advised), they must be supervised and not left alone with the device. Staff are fully responsible for any problems that happen as a result.
- When leaving a computing device unattended, staff must log out or lock the screen to stop others from accessing their account or emails.
- USB sticks or portable hard drives should not be used with the school system as they might have viruses. Staff must not save sensitive or personal data on these devices unless the school has approved and encrypted them.
- If staff use USBs on their home computers, they must make sure their home computer has updated antivirus software to prevent spreading viruses to the school network.
- If staff use a personal computer or device at home for school work, they must not store any sensitive or personal school data unless the device is fully encrypted by IT support and approved by the headteacher.
- The school server and emails are backed up every night. Staff should regularly back up files from their Desktop and Downloads folder, as these may not be included.
- It is the responsibility of the staff to ensure laptops, tablets, iPads, cameras, and other school devices are locked away at the end of the day and not left where they can be seen through windows or doors.
- Do not click on links or open attachments from unknown or untrusted email sources. Report any suspicious, harmful, or inappropriate content or emails right away to IT support or the Computer Lead.
- In the event that your device is lost or stolen, you must inform the school immediately who will advise on the next steps.

Conduct

Staff must…

- Always use the school's computer system in a professional, polite, and legal way that does not harm the school's or their own reputation.
- Not access, use, download, or share illegal or harmful content, such as child abuse images, racist material, or pornography.
- Use or share offensive, rude, racist, sexist, or threatening language or material or make jokes or comments about someone's race, gender, or sexual preference.
- Follow and respect the school's computer security rules and not try to get around them.
- Not damage or harm any school computer or device.
- Not download large amounts of data or store lots of personal files on the school system.
- Not access, copy, or change another person's files without permission.
- Only contact pupils, parents, or carers using school email accounts or systems, and always be professional. These communications should be recorded on CPOMS. Personal phones or email accounts must not be used.
- Ensure that pupil information must is not stored on laptops or taken off school grounds unless for a trip, and only by the group leader which will be kept securely.
- Ask IT support or Computer Lead if they want programs installed onto computing devices.
- Keep all pupil and staff data private, unless required to share by law or school policy.
- Have permission before using someone else's work and follow copyright rules. Music, videos, and other protected materials should not be copied or shared illegally.
- Be responsible for their actions, both in and out of school.

Mobile Phones

- Staff must not use their mobile phones when children are present. Phones should be switched off or on silent and kept out of sight, such as in a cupboard or a bag, during the school day.
- Staff must not charge their phones in the classroom.
- Phones can only be used in the PPA room or staff room during breaks or lunchtime, or with permission from the Headteacher or a senior staff member.
- Children must never be allowed to use staff mobile phones.
- Staff must not use personal phones to take photos or videos of children or to update Seesaw/Tapestry unless the Headteacher has given permission. If allowed, photos must be moved to the school computer system immediately and then deleted from the phone. However, if mobile phones are the only device available and are used to take photographs they should only be used in exceptional circumstances.
- Phones are only allowed to be accessed in classrooms when needing to use two-step verification to access school emails.
- If a member of staff needs to make an urgent personal phone call they can use their phone at an appropriate non-contact time If a member of staff has a family emergency or similar and needs to keep their mobile phone to hand, prior permission must be sought from their phase leader.

Personal Use

The school allows staff to use school computers for personal reasons from time to time, as this can help improve IT skills and support a good work-life balance. This is allowed under the following conditions:

- Staff must still follow this Acceptable Use Policy and all other school rules for staff behaviour.
- Personal use must not slow down or affect the school's computer system.
- Staff laptops must not be used for business or commercial work unless the school gives permission.
- IT support monitors all computer use, whether it's for work or personal reasons. If you access private information, you do so at your own risk.
- Staff must not store personal files on the school system, including:
  - Music
  - Games
  - Videos

- Photos or images

If these types of files are found, staff will be asked to delete them.

Photographs

- Staff must get permission before taking or sharing photos or videos of other staff or children, and must follow the school's rules on using digital images. If images are shared (e.g. on the school website), names or personal details will not be included.
- Photos shared on Seesaw or Tapestry will include a child's first name and first letter of their surname. Parents have been informed and have given permission for this.
- Staff can take photos or videos for educational purposes, but must follow school rules on how these are shared and used. Images should only be taken using school devices. In rare cases where a personal phone is used, the photos must be deleted as soon as possible.

Smartwatches

- Staff are permitted to wear smartwatches at school; however, if the device includes a camera function, it must not be used to operate the camera—either directly or via a connected mobile phone—in accordance with the above guidelines on mobile phone use

Supervision of Pupils

- Pupils must always be supervised when using school computers or mobile devices during lessons.
- Staff should regularly remind children about the Acceptable Use Policy to help keep them and the devices safe.
- Children must not use computing equipment without supervision during break or lunchtime.
- Staff can use 'School Cloud' or 'Vygon' to monitor pupils' work during lessons, and are encouraged to do so.
- All children's mobile phones must be collected at the start of the day and locked away safely. Phones are returned at the end of the school day. Children should not use them during school hours.
- Children should be informed that their computer use is being monitored. Any inappropriate internet searches will be flagged, and parents will be informed of any misuse.
- All staff should teach the children about how to use ICT and the internet safely whenever possible.
- Teacher tablets have staff access only. Children must be supervised when using these and use them at the risk of the teacher.

Use of Social Networking, Websites and Online Forums

Staff should be careful when using social media, even in their own time. Please follow these rules:

- Do not use social media during school time or on school devices.
- Do not add pupils as friends or message them privately on social media, even for school reasons.
- Be careful what you post online. Make sure your comments don't harm your professional reputation or that of the school.
- Unless you have permission, do not post anything that makes it seem like you are speaking for the school.
- Do not mention the school on social media in a negative or inappropriate way.

Use Of Your Own Equipment – Bring Your Own Device

- If you bring your own device to school, it's your responsibility. The school is not responsible for any damage or loss. When not in use, keep it in a safe place.
- Do not store school photos or videos that include staff or children on your personal devices like phones or tablets.
- Do not connect your personal devices to the school's computers or network without permission from IT Support.
- Any staff member, volunteer or student found to be non-compliant with this policy will face disciplinary action.