Willow Wood Community Primary School Policy on the Appropriate Use of Digital Devices and Mobile Phones

1. Purpose

To ensure the safe, respectful, and educational use of digital devices and mobile phones in line with safeguarding responsibilities outlined in Keeping Children Safe in Education 2025, Early Years Foundation Stage Statutory Framework 2025 and the Schools Code of Conduct 2025.

Ofsted have stated that when gathering evidence about the strategic leadership of attendance and behaviour, inspectors are directed to check that leaders:

"*have high expectations of all pupils' attendance, behaviour and attitudes, and design effective policies that communicate these high expectations clearly to all staff, pupils and parents, including expectations related to mobile phones.*"

Therefore, it is expected that staff, pupils and parents adhere to this policy throughout the school day, including during lessons, breaktimes and lunchtimes.

This policy takes into account he guidance document form the Department for Education – Mobile Phones in Schools January 2026.

Mobile phones in schools - GOV.UK

2. Scope

This policy applies to:
- Pupils
- Staff
- Parents, carers, and visitors
- Any digital device used on school premises or during school-related activities

3. Pupils

Mobile Phones

Pupils are not permitted to use mobile phones during the school day, except where they are used for medical reasons e.g. as a diabetic glucose tracker. In these situations, where devices are used for medical reasons, children **MUST** be supervised at all times when using the device. School has a duty under the Equality Act 2010 to avoid disadvantage to a disabled pupil caused by the school's policies and practices. Allowing access to digital devices for health or SEND reasons is a reasonable adjustment and a failure to allow access may be a breach of school's duty. However, allowing flexibility for individuals with

specific circumstances does not mean that these pupils are exempt from all restrictions on the use of their mobile phones or digital devices and school will endeavor to develop practices which enable those pupils to use their mobile phones and devices for a specific purpose at specific times and locations as necessary.

Phones brought for safety reasons must be switched off on arrival and handed in to the class teacher to be stored securely in the locked classroom cupboard. Unauthorized use will result in confiscation and parental contact. Senior leaders in school will regularly check that this policy is being adhered to through the checking of cupboards etc. to ensure that they are locked.

Staff located at the school gates will ensure that children do not use their mobile devices until they are clear of the school gates.

By handing all mobile phones to staff at the start of the school day, all pupils can feel safe on their journey to and from school, while removing digital distractions for the entirety of the school day. It also provides parents with reassurance that their child is safe if they are travelling to and from school independently.

If a mobile device has not been handed in to a member of staff on arrival at school and is located during the course of the day, the school behaviour policy will be enforced and the phone kept safe until it can be collected by a parent or carer. On collection, they will be reminded, alongside the child, of the expectations related to mobile phones and school use.

Children will be taught about the risks that are associated with the use of mobile phones, both in school and more broadly in order to keep themselves and others safe. Pupils will be taught the benefits of having a mobile phone free environment and be encouraged to see such an environment as desirable and valuable.

This policy will be shared with all parents via a text link and via Facebook and the school website to ensure parents are aware of the expectations and school culture and is transparent to all.

Digital Devices

School-issued devices are for educational use only. Pupils must follow the Acceptable Use Agreement. Personal devices are not allowed to be used. On residential visits, mobile phones will not be allowed; especially due to the rise in the use of E-sims. Apple watches (and other technologies of this nature including Garmin etc.) are not allowed in school due to their increased capacity to send external messages and distract learning.

Online Safety

In accordance with KCSIE 2025, pupils will be taught about online risks, including misinformation, cyberbullying, grooming, and inappropriate content. Under the statutory guidance 'Keeping Children Safe in Education (2025)', safeguarding provision in our school must include robust measures to ensure children's safety online and when using digital technology. This means that the school must put in place 'appropriate filters and appropriate monitoring systems' and regularly review their effectiveness, to reduce children's exposure to illegal, inappropriate or harmful content via the school's IT systems. GOV.UK+2GOV.UK+2

Furthermore, the guidance Cyber security standards for schools and colleges requires the use of a correctly configured boundary (or software) firewall and centrally managed, up-to-date anti-malware protection across all school-managed devices and digital services so as to safeguard personal data, maintain the integrity of systems, and prevent unauthorised or malicious access. GOV.UK+1

These measures — filtering, monitoring, firewalls, device-security and regular review — must be treated as core components of our safeguarding framework rather than optional IT extras. In doing so, we help ensure that our children's online experiences while on school premises (or using school-managed equipment) are as safe as their physical environment."

The school will implement DfE-recommended filtering and monitoring systems. Any notifications received alerting the headteacher and SLT to any inappropriate searches or use of the internet will be followed up and appropriate action taken. Notifications for children will be recorded on CPOMS and for staff they will be kept within a monitoring file.

4. Staff

Use of Mobile Phones and Devices

Staff must not use personal mobile phones in the presence of pupils throughout the school day in any circumstances including when in contact areas or during meetings with pupils or parents. This will empower staff to better challenge pupils to meet the school expectations and effectively enforce the prohibition of mobile phones in school. Personal phones must be stored securely in classroom cupboards and these must be locked when children are in the classrooms and used only during non-contact time and in non-contact areas e.g. the

staffroom. In emergencies, staff must inform the office to make them aware of emergency, incoming calls so that they can be alerted. Staff must not use personal devices to take photos/videos of pupils or communicate with them. School-provided devices must be used for work purposes only and kept secure.

If staff use Apple watches, these must be set to airplane mode during teaching time to ensure staff are not distracted by incoming messages or emails. Watches can be taken off airplane mode at breaktimes when not on duty and not used in contact areas. They must be placed back on light mode at the start of the lesson. Any use of Apple watches or equivalent mobile technology in lesson time will be in breech of the staff Code of Contact.

Communication with children and vulnerable adults, by whatever method, should take place within clear and explicit professional boundaries. Employees should not share any personal information with a child, or young person and should not use their personal mobile to communicate with any young person or on a personal level or to take photographs/videos of pupils/students.

School will provide devices such as iPads rather than expecting staff to use their own devices (e.g. on school trips). Staff should ensure that the device is secure (e.g. password/fingerprint protected) so that unauthorised access to data is prevented. Equipment provided by the school should not be used for personal use or shared with family members/friends.

Employees must not give their personal contact details to children, or young people, including their mobile telephone number. Employees must inform the Headteacher or line manager immediately if contacted by a young person on a personal mobile / device.

WhatsApp and Messaging Apps

WhatsApp or similar apps may be used for work-related communication only. Staff must communicate professionally, avoid sharing sensitive data, not contact colleagues outside working hours unless urgent, and not use personal devices for school-related messaging unless authorised. Despite the informal nature of instant messaging, everyone is expected to communicate professionally.

WhatsApp or other group messaging facility should only be used for work-related purposes. They should be used as a convenient way to distribute information to colleagues quickly and efficiently and for colleagues to communicate easily with each other regarding work matters.

Employees should seek consent before adding other employees to a work messaging group. If an employee is uncomfortable joining, their decision should be respected. Other means of communication should be considered to make sure they stay informed and included. It is not acceptable to purposefully exclude certain colleagues from work related group chats or to set up groups designed to abuse or belittle other employees. This would be in breach of the staff Code of Contact.

All communications via WhatsApp or other instant messaging apps must be polite, respectful, free from discrimination and nothing which may be reasonably considered inappropriate, demeaning or inflammatory should be sent. Employees should not:

- Engage in 'banter' or gossip.
- Use inappropriate language, including swearing and discriminatory words.
- Send inappropriate jokes, images or videos.
- Share photos, videos, memes, or similar assets that aren't relevant to work.
- Use the group to express personal opinions or post private messages.
- Make comments about colleagues.
- Voice personal grievances about work, senior leadership, Governors, or with other individuals.

If an employee sends an inappropriate message, it should be addressed immediately. Employees should report any concerns.

Messages sent on WhatsApp can be legally disclosable and employees should not send anything they would feel uncomfortable being made public. Messages should be retained in line with the school's retention policy.

Ex-employees should be removed from any chats or groups as soon as they have left the school.

Employees should not share highly sensitive data or school information via WhatsApp. To ensure GDPR compliance, any personal data shared should be done for a legitimate business purpose. Employees should be mindful of inadvertently sharing confidential information or personal information. This can quite easily happen in a large group where an assumption is made that something is common knowledge at work,

whereas the information may only have been intended to be known by a small group of people.

Employees should avoid communicating in work related messaging groups outside of working hours. All staff, especially, Headteachers should be particularly cautious about contacting employees outside of working hours, especially if they use a personal device and/or a response is requested. Employees are not expected to respond to any messages outside of working hours, unless where the situation is urgent or in an emergency. An email disclaimer stating the above will be placed on the bottom of all email communication to reassure staff.

Where an employee is on long term sickness absence or other long-term leave of absence, consideration should be given (in discussion with the individual) as to whether it is appropriate for them to remain a member of the group during the period of absence.

If an employee has a work device this should be used rather than a personal device.

Communications with parents should only be done via an official school Messenger account and not from personal accounts.

Failure to comply with the expectations set out above will be investigated in line with the school's Disciplinary policy and could result in disciplinary action, including the possibility of summary dismissal.

Any damage incurred to school devices when not in school is the responsibility of the staff member to repair it using only school approved technicians (Oneit). They will be responsible for all costs incurred.

Social Media

Staff must not befriend pupils or former pupils online, share confidential school information, or air grievances about the school on social media. All online activity must reflect the school's values and safeguarding standards.

All employees are expected to use social media responsibly so that the confidentiality of pupils/students, staff and the reputation of the school are safeguarded. Employees should be conscious at all times of the need to keep their personal and professional lives separate when using social media. If a child should contact a staff member using social media, this should immediately be reported to the headteacher who will contact parents and speak to the child. The staff member will be asked to review their security settings to ensure they provide an enhanced level of protection.

The web and social networking services i.e. Facebook, X, Instagram, Snapchat etc have an important part in many aspects of school life, including external communications. It is recognised that social media is used by children, vulnerable adults and employees for both work related projects or for personal use. Employees are **personally responsible** for the content they publish on social media, blog or any other form of user-generated media. Please remember that internet content is never truly deleted or private. This means everything that is published will be visible to the world indefinitely. Employees should be sure that they want what they're posting to be in the public domain with their name on it indefinitely. **If in doubt, don't post**.

Employees are advised to keep profiles safe by not showing their job title, place of work or work/home email address. Employees should be cautious declaring their status / relationship status / sexual orientation as young people may challenge them i.e. online dating. Employees should ensure that they manage and understand the privacy settings on their social media.

Employees should not befriend children/young people where their only relationship is one formed through an employees' professional role. Employees should not use internet or web-based communication channels to send personal messages to a child/young person.

Photographs, videos or any images of pupils or students, vulnerable adults or colleagues should not be published on personal social media platforms without prior permission of parents/carers /colleagues and the school. Permission should be gained through existing school procedures.

Employees must avoid airing their personal grievances about work on social media. This has the potential to damage the reputation of the school, following appropriate investigation, could involve disciplinary action. If an employee does have an issue or grievance they want to raise, this should be done internally so it can be properly addressed.

Employees are expected to respect their audience. This goes without saying, but employees must not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the workplace. Where this is encountered from parents on social media platforms, this must be bought to the attention of the headteacher or designated safeguarding leads so that they can discuss this with parents.

Employees must not use their school email address to sign up to social media sites. Social media must not be used for work related communication, unless authorised to do so via the school's official social media sites. Internet use during working hours is strictly for business not personal use.

Any form of personalised social media networking that is found to reveal confidential information about the school, information relating to a pupil or student, attacks on or abuse of a colleague or 'customer' of the school, or constitutes a conflict of interest, or is in breach of the Code of Conduct may lead to a disciplinary investigation and appropriate action.

5. Parents and Visitors

Parents have an important role to play in supporting school's policy on mobile phones. Willow Wood Community Primary School will ensure that the policy is clearly explained to parents, including the rationale and expectations around its implementation. Parents are encouraged to support the school and explain the policy at home as appropriate; including the risks that come with mobile phone usage. Where parents need to contact pupils over

the course of the school day, they should contact the office who will ensure that all relevant and important messages are passed on to pupils before the end of the school day.

Mobile phones should be on silent during school visits and they are not allowed to be used around the school building or outdoor areas. Mobile phones must be contained in a bag or pocket. Parents will be challenged by staff if they are seen to be using a personal device on school premises. Photos/videos may only be taken with explicit permission from the Headteacher.

At performances and school events, parents and visitors will be made aware of the expectations re taking photographs and staff will endeavor to take individual photographs of children for parent's sole use. These will be sent as soon as practicable after the event. This will also apply to residential visits such as Derwent Hill.

Parents should only use official communication channels to contact staff.

6. Safeguarding and Digital Safety

In line with KCSIE 2025 and the Code of Conduct, technology is recognised as a significant component in safeguarding and wellbeing issues. In accordance with Keeping Children Safe in Education (2025), we understand that "safeguarding and promoting the welfare of children" includes protecting children from maltreatment both inside and outside of school, including online harms. Risks include exposure to harmful content, online abuse and exploitation and peer-on-peer abuse via digital platforms. The school will use appropriate filtering and monitoring, ensure staff understand their roles in digital safeguarding, and promote a child-centered approach to digital safety. Digital safety lessons will form a large part of the computing curriculum.

In line with our Acceptable Use Policy, it is integral to our wider safeguarding framework: all activity on school-managed networks and devices, including internet use, must comply with this policy. We accept our responsibility to protect children from the four key categories of online risk identified in KCSIE:

- Content (e.g. exposure to harmful or inappropriate material).
- Contact (e.g. harmful or exploitative interactions).
- Conduct (e.g. cyberbullying, sharing inappropriate images).
- Commerce (e.g. scams, financial exploitation). GOV.UK+1

The headteacher and deputy headteacher will receive alerts whenever a blocked site has been accessed. This will be investigated and appropriate actions taken, the outcomes of which will be recorded on CPOMS for children and placed in a file for staff.

7. Misinformation, Disinformation and Conspiracy Awareness

As digital information becomes increasingly complex, children are more frequently exposed to misinformation (false information shared without intent to harm), disinformation (false information deliberately created to mislead), and conspiracy content. In line with the online-safety expectations set out in *Keeping Children Safe in Education (2025)*, our school recognises that these forms of harmful or misleading content can influence children's beliefs, behavior, wellbeing and sense of safety.

Within computing and digital learning, pupils may encounter manipulated images, misleading videos, AI-generated content, false narratives or material designed to provoke strong emotional responses. Such content can contribute to online manipulation, fear or distress, discriminatory attitudes, extremist views, or unsafe online conduct.

To safeguard pupils and promote responsible digital citizenship, this Acceptable Use Policy requires that:

- Pupils learn how to recognise, question and critically evaluate online information, including sources that seem authoritative or "viral."
- Pupils must not create, share or promote misleading content, conspiracy material, doctored media or information intended to cause harm, fear or confusion.
- Staff model critical digital literacy skills and support pupils in distinguishing fact, opinion, bias, satire and deliberate manipulation.
- Any concerns about a pupil's engagement with harmful online narratives, including extremist or radicalising content, must be reported immediately through the school's Child Protection Policy and safeguarding procedures.
- School-approved teaching materials, filtering and monitoring systems will be used to reduce exposure to harmful misinformation and to provide safe, age-appropriate environments for research and digital learning.

Our approach ensures that children develop the skills and confidence to navigate online information safely, responsibly and ethically, reinforcing our commitment to safeguarding in a digital world.

8. Use of Artificial Intelligence (AI) and Online Safety

The increasing availability of Artificial Intelligence (AI) tools, online platforms and automated content-generation systems forms an important part of children's digital world. In line with Keeping Children Safe in Education (2025), our school recognises that safeguarding now includes protecting pupils from online risks associated with AI. These risks sit across KCSIE's four areas of online safety: content, contact, conduct and commerce.

AI systems may expose children to:
• Inaccurate or harmful content generated by algorithms (e.g., misinformation, inappropriate responses).
• Unregulated contact through AI-powered chats or automated messaging tools, which may mimic real users.
• Risks related to conduct, including the creation or sharing of inappropriate images, deepfakes, or material that could contribute to bullying.
• Commercial risks, where AI systems encourage data sharing, in-app purchases or engagement with unsuitable services.

For these reasons, our Acceptable Use Policy sets clear expectations for how AI-enabled tools may be used in school.

- Pupils may only use age-appropriate, school-approved AI platforms under staff direction.
- They must not enter personal information, upload images of themselves or others, or use AI systems to generate harmful, offensive or misleading content.

9. Com Networks

Community 'COM' Networks are online groups involved in child sexual abuse, cybercrime and offline violence. These networks are dynamic and often overlap across the threats, although not every case will involve all three. The majority of those involved (victims and perpetrators) are predominantly but not always children under the age of 18. Com Networks are active on virtually all social media and online gaming platforms but primarily operate on Discord and Telegram which are popular communication platforms. The types of harm caused, including grooming, extortion, cyber-attacks, and in-person violence. Offenders seek out vulnerable and susceptible victims (children and adults) to groom, manipulate and exploit. Individuals may be particularly vulnerable to such targeting if they use online forums providing help and advice for:

- Mental health disorders
- Neurodiversity
- Body image disorders

- Self-harm and suicide
- Sexual orientation and gender identity
- Sexual and/or physical abuse
- Substance misuse

All staff and volunteers need to be aware of potential behaviours or indicators that a young person may show if they are involved in a Com group:

- Self-harm (of note, cutting numbers/letters /symbols, or to the breasts/genitalia) known as cut signs or fan signs).
- Numbers, letters symbols written in blood on walls knowns as 'blood signs'.
- Interest, possession or promotion of extreme themes or materials.
- Disengaging from education.
- Obsession with new online friends.
- Unexplained injuries or death of pets.
- Unexplained injuries to siblings.
- 'Doxing' (the malicious sharing of private or identifiable information) and/or 'Swatting' (abuse of the 999 system to trigger an armed police response to a location).
- Unexplained money or gifts.
- The use of encrypted or fringe communications platforms (Discord and Telegram).
- Individual has an intense interest in cyber activities.
- Individual is in possession of advanced software that does not reflect typical use (i.e. TAILS).
- Individual has an advanced understanding of digital technologies, hardware, and software.
- Individual has skills in specialized and varied software, programming, and network configuration (i.e. knowledge of how to use Kali-Linux and/or ability to write in code).
- Individual has a known history of hacking, SIM swapping, swatting, DDOS, online fraud (use of compromised credit cards).
- Unexplained wealth – where individual is in possession of items whose value is disproportionately high to family or individual income.
- Interest and advanced understanding of cryptocurrency.

Willow Wood Community Primary School will:

- Raise awareness among staff about the risks, including recognising signs of exploitation, cybercrime, and online harms.

- Follow local safeguarding procedures when concerns arise.
- Provide pupils and families with clear instructions on reporting online safety issues.
- Encourage pupils to seek support from trusted adults in school.
- Share guidance with parents on maintaining children's online safety.
- Ensure ICT and acceptable use policies and risk assessments are current and comprehensive.

Professionals should be aware that due to this threat and during their interactions with a child or young person, they may experience behaviors, disclosures or material that is distressing and outside of the 'norm'. Any well-being concerns that you have about yourself or colleagues should be discussed with the headteacher.

10. The Use of Sanctions

Willow Wood Community Primary School will follow Department of Education guidance when implementing any sanctions related to breeching the Mobile Phone and Digital Devices Policy for staff, parents and pupils. For pupils, this could mean confiscation of the device. This could include instances where a mobile phone has been used in school by a pupil or a phone has been heard ringing in a bag. The law protects staff from liability in any proceedings brought against them for any loss or damage to items that they have confiscated as a sanction, providing that they have acted lawfully. Staff should consider whether confiscation is proportionate and consider any special circumstances relevant to the situation.

Headteachers are backed by the DfE to confiscate mobile phones and similar devices if they consider it to be proportionate and for whatever length of time they consider to be proportionate. School must consider the circumstances around confiscation such as whether a sanction could achieve the same result as confiscation or the pupil's individual circumstances such as age or SEND status. Confiscation can be an effective deterrent for individual pupils or all pupils in the school.

11. Monitoring and Review

This policy will be reviewed annually by the Senior Leadership Team. Updates will reflect changes in statutory guidance, including future versions of KCSIE and the Code of Conduct. Feedback from pupils, staff, and parents will inform revisions.

All staff should consistently enforce the school's policy on the use of mobile phones and digital devices.

Policy written: March 2026

Policy review : March 2027