Hamsey Green Primary School

Online Safety Policy

Hamsey Green Primary School

Acorns Nursery

Policy Reviewed: September 2025
Next Review Date: August 2026
Reviewer: Mr John Boffa (Deputy Head)

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright

Commerce

- Online gambling
- Inappropriate advertising
- Phishing
- Financial scam

The Policy will be communicated by:

- The policy will be communicated to staff/pupils/community in the following ways:
- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school. This should be done as part of the annual safeguarding training with staff.

Communication of the policy to pupils.

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their e-safety education.

Communication of the policy to parents and carers.

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety policy in newsletters and on the school website.
- Parents will be offered online safety training annually

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

•Ensure that they have read and understand this policy

•Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

•Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Handling of Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequence of internet access.

Handling complaints

- Complaints of internet misuse will be dealt with according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Social networking

- Staff, Volunteers and Contractors
- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Any school approved social networking e.g. Facebook and Twitter will adhere to the policy that we do not put pupils, staff or parents on to social media without their agreement.

Use of Social media including the school learning platform.

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services e.g. Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Publishing pupils' images and work.

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in the Surrey Safeguarding Children Board guidance on using images of children.

Published content – school website and social media.

- The contact details will be the school address, email and telephone number. Staff or pupil's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Pupils:
- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- Parents:
- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- They are reminded that they need to ask permission before uploading photographs, videos or any other information about other people

Mobile phones, tablets and other mobile devices

- Mobile devices brought into school are entirely at the staff member, students (who are in year 5 and above and walk home alone) & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices are not permitted to be used in certain areas within the school site.

- All pupil mobile devices are collected in by the class teacher at the start of the day and handed in to the school office. They can be collected from the office once the child has been dismissed
- No images or videos should be taken on mobile devices
- All members of staff and visitors working in classrooms are requested to keep their phones switched off and securely stored away. Midday Meals supervisors are not allowed mobile phones whilst on duty.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- To carry out the search the school must:
    - Have "reasonable grounds for suspicion"
    - Have two adults present
    - Stop short of accessing cloud accounts
    - Not view illegal content themselves (e.g., indecent images of a child)

- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Staff may use their phones during break times. Members of staff should ensure that anyone wishing to contact them urgently should do so via the school office stating the urgency of the matter. The Headteacher may give permission for a member of staff to return a call in these circumstances.
- Staff should only use their phones in areas where there are no pupils, the staffroom, offices, PPA area and only in classrooms outside of pupil hours.

Protecting Personal data.

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and personal data on and off site, remote access to school systems.

Policy – authorising access.

- All staff must read and sign the Staff AUP before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At KS1 access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At KS2 access to the internet will be with teacher permission with increasing levels of autonomy.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform (if used).
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
- The class teacher/SLT will determine how emails from pupils to external bodies is presented and controlled.

Community use of the internet

- Members of the community and other organizations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.
- Secondary pupils must apply for internet access individually by agreeing to comply with the student AUP.
- People not employed by the school must read and sign as a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow the use of technology by their pupil.

Managing access and security

The IT network manager will provide managed internet access to its staff and pupils in order to help pupils learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- The security of school IT systems will be reviewed regularly.
- All staff members who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

<u>Child Protection Procedures</u>

If any of the concerns are raised that are related to child protection the school and any adult is responsible to report it to a DSL using CPOMS. In this case procedures from the Safeguarding Policy should be followed. As shown below:

The following procedures apply to all staff working in the school and will be covered by training to enable staff to understand their role and responsibility.

The aim of our procedures is to provide a robust framework which enables staff to take appropriate action when they are concerned that a child is being harmed or abused or is at risk of harm or abuse.

The prime concern at all stages must be the interests and safety of the child. Where there is a conflict of interest between the child and an adult, the interests of the child must be paramount.

All staff are aware that very young children and those with disabilities, special needs or with language delay may be more likely to communicate concerns with behaviours rather than words. Additionally, staff will question the cause of knocks and bumps in children who have limited mobility.

If a member of staff suspects abuse, spots signs or indicators of abuse, or they have a disclosure of abuse made to them they must:

1. Make an initial record of the information related to the concern.

2. Report it to the DSL immediately.

3. The DSL will consider if there is a requirement for immediate medical intervention, however urgent medical attention should not be delayed if the DSL is not immediately available.

4. Make an accurate record on CPOMS (which may be used in any subsequent court proceedings) as soon as possible and within 24 hours of the occurrence, of all that has happened, including details of:

Dates and times of their observations

Dates and times of any discussions in which they were involved.

Any injuries

Explanations given by the child / adult

Rationale for decision making and action taken

Any actual words or phrases used by the child

5. The records must be signed and dated by the author or / equivalent on electronic based records

6. In the absence of the DSL or their Deputy, staff must be prepared to refer directly to C-SPA (and the police if appropriate) if there is the potential for immediate significant harm.

Following a report of concerns the DSL must:

1. Using the SSCB Levels of Need, decide whether or not there are sufficient grounds for suspecting significant harm, in which case a referral must be made to the C-SPA and the police if it is appropriate.

2. Normally the school should try to discuss any concerns about a child's welfare with the family and where possible to seek their agreement before making a referral to the C-SPA. However, this should only be done when it will not place the child at increased risk or could impact a police investigation. The child's views should also be taken into account.

If there are grounds to suspect a child is suffering, or is likely to suffer, significant harm or abuse the DSL must contact the C-SPA. By sending a Multi-Agency Referral Form (MARF) by email to: cspa@surreycc.gov.uk or contact the C-SPA on 0300 470 9100. If a child is in immediate danger and urgent protective action is required, the Police (dial 999) must be called. The DSL must also notify C-SPA of the occurrence and what action has been taken

3. If the DSL feels unsure about whether a referral is necessary, they can phone the C-SPA to discuss concerns

4. If there is not a risk of significant harm, the DSL will either actively monitor the situation or consider the Early Help.

5. Where there are doubts or reservations about involving the child's family, the DSL should clarify with the C-SPA or the police whether the parents should be told about the referral and, if so, when and by whom. This is important in cases where the police may need to conduct a criminal investigation.

6. When a pupil is in need of urgent medical attention and there is suspicion of abuse the DSL or their Deputy should take the child to the accident and emergency unit at the nearest hospital, having first notified the C-SPA. The DSL should seek advice about what action the C-SPA will take and about informing the parents, remembering that parents should normally be informed that a child requires urgent hospital attention.

7. The exception to this process will be in those cases of known FGM where there is a mandatory requirement for the teacher to report directly to the police. The DSL should also be made aware.

Internet use

The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others safety.

All communication between staff and pupils or families will take place using school equipment and/or other school accounts.

Pupils will be advised not to give out personal details or information which may identify their location.

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in online safety / digital literacy is therefore an essential part of the school's / academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

- **A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / pupils should be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**

- *Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.*

- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Cyber Bullying and online sexual harassment

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

- No form of bullying is accepted at Hamsey Green Primary School and any behaviour demonstrated as cyber bullying will be treated the same way as in school (refer to the Behaviour for Learning Policy).
- Any form of sexual harassment online such as sharing nude and semi-nude images and/or videos (consensual and non-consensual) of U18 is a criminal offence. Please refer to P36 of the Child Protection and Safeguarding Policy.

Artificial intelligence (AI)

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.
- We recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI

is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

- We will treat any use of AI to bully pupils in line with our behaviour policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

Appendix

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it • The messages I send and write will be polite and responsible. **I will not:** • Access websites unless my teacher has expressly allowed this as part of a learning activity • Access other people's files. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online or using entering information. • Search for or create links to inappropriate material. • Log in to the school's network using someone else's details • Install software on school computers. • Use the school system for gaming, gambling, shopping or uploading videos or music. **Personal Devices:** The school cannot accept responsibility for loss or damage to personal devices • It is not permitted for pupils to use Mobile phones during the school day. Phones should be handed to the school office at the start of the school day. • E-readers, Kindles and cameras should only be brought into school with permission from a teacher and used only with permission. **I agree that the school will monitor the websites I visit. I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour wherever their location. If the activities are illegal this may be reported to the police.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	

Signed (parent/carer):	**Date:**