Hamsey Green Primary School

Online Safety Policy 2017

Hamsey Green
Primary School

When the policy will be reviewed:

The e-safety policy is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour and anti-bullying, safeguarding, data handling and the use of images.

- **The school will form an e-safety committee and will appoint an E-safety coordinator. In many cases this will be the Designated Child Protection Coordinator as the roles overlap.**
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The E-safety Policy and its implementation will be reviewed annually. The next review is due in November 2018.
- The E-safety Policy was revised by: Mr J Boffa – Assistant Headteacher
- It was approved by the Headteacher: November 2017
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, tablets and hand held games consoles used on the school site.

The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil

<u>The main areas of risk for our school community can be summarised as follows:</u>

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

<u>The Policy will be communicated by:</u>

- 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.

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 behavior 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 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 has a separate Social Media Policy.

- 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/School Business Manager 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 (Purple Mash).
- 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 & 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. Staff mobiles devices may be searched at any time as part of routine monitoring.
- 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 – authorizing 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 school 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.

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.