PRIOR HEATH INFANT SCHOOL
POLICY & PROCEDURES STATEMENT

TITLE: Online Safety Policy **DATE: March 2017**
REVIEW: March 2018

APPROVED/MONITORED BY: **Children & Learning Committee**
AGREED BY: **Whole school staff & governors**

Overview

The opportunities provided by the Internet are tremendous, both within school and outside. Online safety is part of the school's safeguarding responsibilities. We have an education safeguarding responsibility to educate children about the benefits, risks and responsibilities of computing. Our online safety policy has been written by the school, using Surrey County Council and Government guidance. The online safety policy and its implementation will be reviewed annually. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images.

Using this policy

- The school online safety co-ordinator is Rachel Bates. The online safety co-ordinator will update staff on developments in online safety as needed.
- Our online 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 online safety policy was revised by: Rachel Bates
- It was approved by the Governors: March 2017
- The online safety policy and its implementation will be reviewed annually. The next review is due: March 2018.
- The online 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, mobile phones, tablets and hand held games consoles used on the school site.
- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access is provided by Surrey County Council through the UNICORN contract and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through regular online safety lessons.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. pressing the Hector Protector button.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to 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.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Teachers are responsible for ensuring the suitability of content on sites they request to be unblocked.
- 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 school accounts.

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

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.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content e.g. school web site, school social media accounts

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

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 Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media

- 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. At Prior Heath, pupils do not access social networking sites in school.
- 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.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the online safety policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling Policy. It covers access to pupil and staff personal data on and off site and remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff Acceptable Use Policy' (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 Prior Heath, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials**.**
- People not employed by the school must read and sign a Visitor AUP before being given access to the internet via school equipment.
- If parent helpers are asked to support pupils with equipment that accesses the internet, a Visitor AUP will be completed.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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 consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt with according to the relevant school policy e.g. the school behaviour policy, anti-bullying 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 schools' behavior policy.

Community use of the Internet

- Members of the community and other organisations using the school internet connection will have signed a Visitor AUP/Code of Conduct so it is expected that their use will be in accordance with the school online safety policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the online safety rules in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about online safety as part of their online safety education.
- Online safety education takes place half termly.

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training on an annual basis

To parents

- The school will ask all new parents to sign the parent/pupil agreement when their child joins the school.
- Parents' and carers' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be provided with online safety information annually through the year group information meetings for parents and newsletters.

Responsibilities

The Computing Co-ordinator, Miss Bates, carries out the role of Online Safety co-ordinator and will review the online safety policy annually.

The school staff are responsible for promoting the online safety policy.

Appendix 1

Mobile Technology Guidance

General use of mobile phones

- Mobile phones and personally owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school such as the toilets.
- Personal mobile devices will only be used during lessons with permission from the Headteacher.
- The sharing of images or files with other mobile devices i.e. via Bluetooth or other apps is not allowed.
- No images or videos should be taken on mobile phones or personally-owned mobile devices.

Pupils' use of personal devices

- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Staff use of mobile phones and personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting pupils, parents or those connected with the family of the student.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Mobile phones and personally-owned devices should be switched off or switched to 'silent' mode and left in a secure place in the classroom during lesson times.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- Staff use of mobile phones during the school day will normally be limited to the mid-morning break, the lunch break and before and after school.
- If any staff member has a family emergency or similar and is required to keep their mobile phone to hand, prior permission must be sought from the Headteacher.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Staff should never contact students from their personal mobile phone or give their mobile phone number to students. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
- Staff should never store parents' or pupils' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.

- Staff should never send or accept from anyone texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, preferably the online safety co-ordinator or DSL should be contacted.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.

Parent Helpers and Visitors

Parent helpers and visitors who are in school during the school day or helping on school trips are made aware of the following:

- Mobile phones and personally owned devices may not be used and should be switched off (or silent) at all times.
- Personal mobile devices may only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices.

Parents

Parents are expected to only use mobile devices for urgent communication when on the school premises and we would prefer them not to use their phones at all while at school.

However, we do allow parents to use mobile devices to photograph or video school events such as the Christmas production and sports day. We insist that parents do not publish any images (e.g. on social networking sites) that include children other than their own. Surrey County Council guidelines on photographic images are included in the Harvest and Christmas newsletters. Parents have to indicate that they have read and accepted these before tickets are issued for the Christmas production.