KENTS HILL JUNIOR SCHOOL

Kents Hill Junior School Online and E-safety Policy

1. **Roles and responsibilities.**
   2.1. All staff
   2.2. Designated Online Safety coordinator
   2.3. Designated DSL

2. **Related Policies and documents**
   2.4. Acceptable Use Policy
   2.5. Behaviour policy
   2.6. Code of Conduct Policy
   2.7. Home school agreement
   2.8. Keeping Children Safe in Education (DfE)

3. **The Curriculum Network**

4. **Curriculum Network Use and Behaviour Policy**

5. **The Internet**
   5.1. Online safety in the curriculum
   5.2. Management of Internet Access.
   5.3. Authorising internet access and use of internet services.
   5.4. Social Networking Sites
   5.5. Pupil use of web based subscription resources
   5.6. Child Protection
   5.7. Online Safety and parent/carer engagement
   5.8. Using the internet to enhance teaching and learning across the curriculum.
   5.9. Internet searching skills.
   5.10. Understanding the internet.

6. **Pupil images and pupil work.**

7. **Mobile phones**

8. **Managing emerging technologies and online safety**

1. Roles and responsibilities.

1.1. All Staff

All staff have a responsibility to apply this policy with regard to child protection, school behaviour policy and teaching the curriculum, which includes online safety. They must report any online safety concerns to the online safety coordinator, or in the case of child protection, follow child protection procedures.

1.2. Designated online safety coordinator

The named online safety co-ordinator is Hannah Nash.

1.3. Designated Safeguarding Lead

The DSL is Hannah Nash; the Deputy DSL is Joanne Parks.
The named LADO (South) is Mechelle de Kock(tel: 0845 606 1212**,** email: childrens.safeguarding@essex.gov.uk)
https://schools-secure.essex.gov.uk/pupils/Safeguarding/Managing_allegations_in_the_Childrens_Workforce/Pages/ManagingAllegationsInTheChildrensWorkforce.aspx

Senior Management and Governors are updated by the Head/ Online Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to online safety.

2. Related Policies and documents

Digital technology use is ubiquitous in school by all members of the school community. For this reason online and e-safety cannot be seen in isolation, and so is reflected in the following documents, Acceptable Use Policy Behaviour Policy, Code of Conduct Policy, Home School Agreement and Keeping Children Safe in Education (DfE). This online and e-safety policy document highlights where sections of those documents referred to above have specific relevance to online and e-safety, and addresses those areas where they are not, i.e. the management of the curriculum network and the curriculum.

3. The Curriculum Network

The school uses an Ergo supplied "Free2Teach" client server network. Pupils and staff have their own user area on the curriculum network. Teaching staff are provided with their own laptop and educational tablet. The appropriate use of these facilities for staff is covered in the Code of Conduct policy, sections 7 and 8. For pupils there are designated laptops, desktops and tablets for each year group. Pupils have access on the school's server to their own personal user area, a shared class area, a shared school area, a suite of pre-selected programs and the internet.

Pupils use the curriculum network to support their learning across the curriculum. Pupils are taught about networks, the IT skills necessary to create folders and rename and copy files to different folders, enabling them to use the network more fully. During Year 6 passwords are introduced for pupils, alongside an input regarding online safety.

The main area, although not exclusively, of concern regarding pupils' online and e-safety comes from the use of the internet and the services it provides. This is reflected in this online and e-safety policy.

4. Curriculum Network Use and Behaviour Policy

The following reinforces the school Acceptable Use and Behaviour Policy in an e-safety context:

- Pupils intentionally interfering with other pupils' work, either of the pupils while they are working, or of files they have saved in a shared location, falls within the school behaviour policy.(e.g. pupils are given 1 warning.)
- Unless given express permission by their teacher, pupils are not to attempt to logon to other pupils' user areas.
- Pupils intentionally destroying or damaging equipment or being clearly careless with equipment falls within the school behaviour policy (e.g. peeling off labels, misuse of CD drives, slamming laptop lids down, removing keyboard keys, or continuously hitting random keys.)
- Accessing programs or the internet against the specific instructions of the class teacher falls within the school's behaviour policy.

5. The Internet

5.1. Online safety in the curriculum

Safe use and understanding of the Internet is a requirement of the National Curriculum for England, as well as being a vital tool for staff. The School's curriculum provides varied and repeated opportunities to use the internet for structured and meaningful activities. This promotes pupils' skills, experience and understanding of the internet and its services enabling them to become discerning and competent users of the technology, more able to protect themselves. Pupils are educated to understand:

- they should never give out personal details of any kind which could identify them or their location
- to never meet up with someone they have only met on line
- to be cautious when accepting texts, e-mails etc. from unknown sources
- to understand that some information may not be reliable
- to tell an adult if at any point they are uncomfortable, worried or unhappy about anything they have experienced online.

This is achieved via:

- specific online safety assemblies with follow up class teacher led lessons
- inputs by class teachers at key points during pupils' use of the internet
- reminders and references in all classrooms regarding online safety in the form of posters and displays.

The school uses the S.M.A.R.T. acronym with the pupils (Safe, Meeting, Accepting, Reliable, Tell).

5.2. Management of Internet Access.

Access to the internet via the curriculum network is provided by the Essex Schools Broadband Subscription Service, allowing different levels of filtering and security dependant on user (i.e. restricted access levels for pupils). For more information see https://schools-secure.essex.gov.uk/admin/Broadband/School%20Services/Pages/InternetFilteringSecurity.aspx.
Laptop and desktop devices also have anti-virus software installed on them.

5.3. Authorising internet access and use of internet services.

Pupils' access to the internet is only allowed under adult supervision.
When pupils need to use particular internet services (Skype, e-mail, educational social networking sites etc.) for a topic or learning objective, staff first consult with SLT regarding the approaches to be taken.

5.4. Social Networking Sites

Pupils' use of social networking sites is blocked. This is for all pupils, and will remain so unless a specific use is approved.

5.5. Pupil Use of web based subscription resources

At present pupils use one web based subscription programs for their learning, MyMaths. This is password protected and closely monitored by staff.

5.6. Child Protection

Pupils attempting to access websites that are sexually explicit, racist or promoting extremist views[1] will be referred immediately to the DSL or Deputy DSL (Designated Safeguarding Lead) using the school's child protection reporting system, or the LADO (L.A. Designated Officer if appropriate). If the school becomes aware that pupils may be accessing these types of sites outside school, this will also to be referred to the DSL or LADO.

Pupils accessing the internet, inside or outside school, to bully other pupils will be referred to the DSL using the school's child protection reporting system. Incidents of pupils who report they have been cyber bullied will be recorded in the same way.[2]
If a pupil discovers any sites he/she is worried, uncomfortable or upset by they should inform the member of staff supervising them at that time, who will follow the school Acceptable Use Policy for such matters. ("If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the online safety co-ordinator.")

---

[1] *DfE Keeping children safe in education. Statutory guidance for schools and colleges 2016 Prevent Strategy*
[2] *DfE Keeping children safe in education. Statutory guidance for schools and colleges 2016 Types of Abuse and Neglect*

5.7. Online safety and parent/carer engagement

The school's website http://www.kentshilljuniorschool.co.uk/keeping-safe/online-safety provides clear information for parents and carers on how to keep their children e-safe. Workshops for parents/carers are held once a year on how to keep their children e-safe.

5.8. Using the internet to enhance teaching and learning across the curriculum.

Staff use the internet to support their teaching, often in order to provide a multimedia input. Staff plan for pupils' use of the internet to support learning objectives from across the curriculum.

5.9. Internet searching skills.

The school has 'Internet Research', a SoW for teaching pupils' internet searching skills. Staff incorporate this into the term or half term curriculum areas the children are studying. The scheme of work progresses from how to bookmark a web page to evaluating sites by understanding which sites can be thought of as an authority. Integrated use of the internet in this way promotes purposeful use of the internet, an understanding of bias, educating pupils to become more discerning about the appropriateness of information they encounter on websites.

5.10. Understanding the internet.

Pupils are taught about networks, the internet and the services available via this technology (e.g. social networking, the world wide web, e-mail etc.) as part of the Computer Science short course. The online safety dimension the technology brings is taught and reinforced to pupils at this time.

6. Pupil images and pupil work.

The school provides devices for taking images.

The school uses images of pupils' and pupil work. The correct use of images (and any other school data) by staff is clearly stated in the Code of Conduct policy. This includes not using their own devices; the school has a strict policy regarding publishing of any images, and always ensures parent/carer permission has been granted.

Pupils can also take images as part of their learning. Where the school or individual staff member feel it would be beneficial, the opportunity to reinforce school behaviour policies with regard to respect for others, educate regarding online safety and personal data, online safety and cyber bullying around the topic of images and the internet, they will do so.

7. Mobile phones

Mobile phone use by pupils during formal school time is not allowed. Year 6 pupils may bring their phones to school, but hand them in at the beginning of the day, for collection at the end of the day. Pupils have access to the school phone if required.

8. Managing emerging technologies and online safety

New technologies are evaluated for education benefit and assessed for risk before use in school.