Ravenscourt Park Preparatory School

e-Safety Policy

1. Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. E-Safety covers issues relating to children and young people, as well as adults, and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

This e-Safety policy sets out how the school plans to develop and establish its' e-Safety approach and to identify core principles, which all members of the school community need to be aware of and understand. It works alongside the school's Safeguarding Children Policy to ensure all members of the school community are kept safe.

The policy and the procedures will be reviewed annually by the Head of Computing. Changes or additions will be reported to the relevant sections of the school community.

2. Teaching and Learning

Internet use is part of the curriculum and is a necessary tool for learning. The school has a duty to provide students with quality Internet access as part of their learning experience, to enable them to access a wealth of online resources and enrich their learning. Pupils need to learn how to evaluate Internet information and to take care of their own safety and security. The purpose of the Internet in school is to help raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Kew House School and Kew Green School and
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

The school's Internet access is designed to enhance and extend education. The eSafety curriculum combined within the Computing curriculum and the pupils Acceptable Use Policy (AUP) will teach children what Internet use is acceptable and what is not, and give clear objectives for Internet use. The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

Staff will guide pupils to particular sites that support the learning intention and are appropriate for the age group being taught. Random searches on the Internet are not productive or appropriate. Pupils will be educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?
Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They will use age-appropriate tools to research Internet content. The evaluation of online materials is a part of teaching and learning in Computing lessons and will become part of other lessons with the introduction of handheld devices. At this point it will be viewed as a whole-school requirement across the curriculum.

How will pupils learn about e-safety and responsible use of technology?
Pupils learn about e-Safety and responsible use of technology through the e-Safety scheme of work which has been incorporated into the Computing Curriculum as part of digital literacy. Children learn about the SMART rules and in PHSE lessons and Anti-Bullying week focus on the dangers of cyber bullying. Year 2 - 6 attend an Internet safety workshop provided by an outside specialist provider such as Childnet International. This raises the profile of internet safety for these year groups and prepares Year 6 for secondary school and focuses on responsible use and develops their understanding and the implications of their digital footprint.

3. Managing Information

How will information systems security be maintained?
The school server is located securely and physical access to it is restricted. It is managed by Doherty Technical Services Ltd who ensure that the server operating system is secure and is kept up to date. Sophos antivirus protection is installed across the school network and updates three times a day. Access to the Internet by wireless devices not joined to the school network, e.g. visitor computers, mobile phones etc. is managed by the school's router. A username and password is required to gain Internet access wirelessly and several levels of permission have been set up. Pupils, Staff and Guests all have access appropriate to their needs. Doherty monitor who is gaining access to the Internet via our wireless connection. The school's firewall protects the school community from undesirable sites and content available online. Access, by staff and visitors, to prohibited Internet sites is also logged and monitored by Doherty.

Staff should log off or lock their machines when leaving them unattended. Usernames and passwords to the school system should be kept confidential by members of staff.

How will email be managed?
Pupils may only use school provided email accounts for school purposes. If email addresses are needed they will be created as a class account and with sensitively so as to not give away personal details. Pupils must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Whole-class or group email addresses will be used for communication outside of the school.

Staff will only use official school provided email accounts to communicate with pupils and parents/carers. As stated in the Safeguarding Children Policy, staff will not have email communication with current or past pupils unless another member of staff and the child's parents are copied in. This type of email communication should be kept to a minimum. Staff access in school to personal email accounts is allowed but these accounts may only be accessed during non-direct teaching time. Personal accounts may not be used to fulfil any type of school business. Emails sent to external organisations and parents should be written carefully, in the same way as a letter written on school headed paper would be. The forwarding of chain messages is not permitted.

How will published content be managed?
The school website is a great source of information for all the stakeholders in the school. Publication of any information online will always be considered from a personal and school security viewpoint. The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published. Material that contains key

information such letters to parents or staff school email addresses will be in a section of the website that is password protected. The Headmaster will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Can pupils' images or work be published?
Images or videos published on the school website, that include pupils, will be selected carefully and will not provide material that could be reused, e.g. small pictures of groups of pupils or 'over the shoulder style' photos that do not show faces. Pupils in photographs will be appropriately clothed and written permission from parents or carers will be obtained before images/videos/work of pupils is electronically published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. General statements will be used to describe photos of the children where necessary.

How will social networking, social media and personal publishing be managed?
Access to social networking sites, social media and personal publishing sites is not permitted in school and key sites such as Facebook / Twitter are blocked by the filter.

Children will be taught about the risks posed by these sites, including the consequences of not enforcing privacy settings correctly (Y5 Computing scheme of work). Pupils will also be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published, (Y6 e-Safety workshop). Staff wishing to access such sites for curriculum related materials must gain permission from the Headmaster or Deputy Head.

Outside of school staff should not post or write negative and damaging information about the school or any of its stakeholders, e.g. the Board, the staff, parents, children. Staff are aware that this contravenes school policy and against teaching standards and publishing unsuitable material may jeopardize their professional status. School staff should **not** be 'friends' or connect with pupils on social networking sites or ex-pupils under the age of 18. Staff are expected to keep a 'professional distance' from the parent body of the school and in this respect are strongly advised NOT to enter into social media exchanges with any parents.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?
The school's broadband Internet connection is filtered and managed by the school's technical company – Doherty, using a reputable and effective Fortigate filter. All sites on the IWF (Internet Watch Foundation) are blocked for all users. This filter allows for different levels of filtering for staff and pupils dependent on the login used. The pupil login has the strongest filter applied. However it is important for staff to recognise that filtering is not always 100% effective and inappropriate content may be accessed. Any inappropriate sites accessed must be reported to the Designated Safeguarding Officer or a member of SLT immediately and recorded in the e-Safety Incident Log, which is kept in the departmental folder. Any material that the school believes is illegal will be reported to appropriate agencies such as the local Police or CEOP. Websites which teachers believe should be blocked centrally should be reported to the Head of Computing. Any changes to the level of filtering will be agreed by the Head of Computing.

Children will be supervised when using Internet access. No unsupervised access by pupils to the Internet is allowed. Acceptable Use Policies are in place for staff and pupils and Internet Safety Rules are displayed in the computer suite and in classrooms. Teachers will always evaluate any websites/search engines before using them with their class; this includes websites shown in class as well as websites accessed directly by the pupils or as part of homework. Often this will mean checking the websites, search results etc just before the lesson, due to the constantly changing nature of websites. Children should be directed to websites by shortcuts / links not via a Google search.

Websites such as YouTube that will be used in school assemblies must be checked for inappropriate adverts and film clips. Wherever possible staff should use Teacher Tube instead of YouTube.

How will videoconferencing / Skype and Facetime be managed?
The use of Facetime and other such technologies on handheld devices is not allowed for use by pupils within school, unless connected to a curriculum focus and the express permission of the member of staff teaching that lesson has been given by the Head of Computing. Parents will be informed of curriculum activities involving videoconferences/Skype/Facetime calls by the teacher prior to the activity taking place so that they have the opportunity to ask further questions if required.

When using video conferencing equipment or opportunities, conferences should always be booked as private and not made public if using a third party provider. Staff should always check who has signed into their conference as a guest without a camera would not be visible. Staff should discuss their requirements for any video conferencing with the Head of Computing before embarking on the project to ensure e-safety guidelines and technical requirements are managed effectively.

Not all staff are aware of how Skype or video conferencing works which potentially puts pupils at risk, e.g. Skype's default operating mode is to be turned on when a computer is logged on. Although Skype is on teaching computers as part of Office 365, it is recommended that for this reason skype and video conference only take place in the school hall for use with the large screen and a webcam or in the ICT suite.

How are emerging technologies managed?
Emerging technologies will be examined for educational benefit before use in school is allowed. The safest approach is to deny access until proper thought or examination of the benefits is complete. Although this may seem stringent, using new technologies will change teacher's pedagogy as well as giving pupils access to online material and careful consideration must be given before their introduction, e.g. a pupil using a mobile device to video a teacher's reaction in a difficult situation.

How should personal data be protected?
The Data Protection Act 1998 (The Act) provides a framework to ensure that personal information is handled properly. Under The Act everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets down 8 data protection principles of which one is data should be kept secure. This applies to all staff

Teachers should not save work containing pupil details or data or photos to their desktop if they take their computer/laptop off site. Staff should take all possible precautions to keep USB memory sticks or portable hard disks containing pupil data secure. Should staff wish to work from home, they should ask Doherty to set up a link to the school network from home to avoid taking data out of the building.

4. Policy Decisions

How will Internet access be authorised?
The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff and pupils in Y2 – Y6 will read and sign the School Acceptable Use Policy before using any school ICT resources annually. Teachers should discuss the rules with children in Y1 and Reception classes. Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

In the Lower School pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials via a web link or shortcut, for example when using the iPads. Upper School pupils will have access to a wider range of sites and undertake searches using age-appropriate search engines, once 'safe searching' has been discussed in their e-safety lessons. **Access will always be supervised.**

All visitors to the school site who require access to the Internet should use the wireless guest log on which limits access and is monitored by Doherty.

How will risks be assessed?
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school can not accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the local police. Methods to identify, assess and minimise risks will be reviewed regularly by Doherty and the Head of Innovation/ SLT.

How will the school respond to any incidents of concern?
Staff may report incidents of concern in person or anonymously to the Headmaster. All reported incidents and actions taken will be recorded in the e-Safety Incident Log (stored in ICT departmental folder) or SLT drive if of a confidential nature. The Designated Safeguarding Lead (DSL) will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place the school will contact and escalate the concern to the Police. If the school is unsure how to proceed with any incidents of concern relating to a member of staff, the Headmaster will seek the guidance of the Hammersmith & Fulham LADO.

How will e–Safety complaints be handled?
Complaints about Internet misuse will be dealt with under the school's complaints procedure. Any complaint about staff misuse will be referred to the Headmaster. All e-Safety complaints and incidents will be recorded by the school, including any actions taken, in the e-Safety Incident Log in the ICT departmental folder. All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection / safeguarding procedures. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Cyber bullying be managed?

Cyber bullying is the use of information and communications technology, particularly mobile phones, email, social websites, text messages, cameras and the internet, to deliberately to upset someone else. Cyber bullying can take place outside of the normal school day and be directed towards the victim while he or she is at home. Silent phone calls or abusive texts or emails can be just as distressing as being bullied face to face. Cyber bullying can have a profound effect on a child as the technology allows information (or misinformation) to be distributed widely, instantly and directly to the child's home or mobile device. The victim can feel that there is nowhere available for him to escape from the bullying.

Cyber bullying (along with all other forms of bullying) of any member of the school community is not tolerated. All incidents of cyber bullying reported to the school will be recorded and incidents or allegations of cyber bullying will be investigated thoroughly. Even if the bullying is taking place outside of the grounds of the school, the school will take action against any pupil responsible for using electronic devices to bully another pupil.
The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Sanctions for those involved in cyber bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff are listed in the schools Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

Staff should not use their mobile phone during directed teaching time or in parts of the school shared by pupils during their non-contact time. When in classrooms or teaching children, mobile phones should be turned off or switched to silent. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use work-provided equipment for this purpose.

There are dangers for staff if personal phones are used to contact pupils and or parents. Therefore a school owned phone should be issued for staff to take on school trips and residentials. Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the school in a professional capacity. The school telephone system should be used for such communication whilst onsite. Please refer to the Acceptable Use Policy for further information on sanctions for misuse. Staff who are on offsite school activities, e.g. on a trip, swimming, in the park, may use their own mobile phones to contact the school office or other members of staff.

Electronic devices of all kinds that are brought in to school are the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.

Pupils Use of Mobile phones and Personal Devices

Children in Year 6 may bring a mobile phone to school in the summer term with written permission from their parents. Mobiles should be handed in at the start of the school day and locked away until dismissal time. Some children with the permission of the Learning Support Department use laptops to complete written work. These devices will not be connected to the school's Internet connection. In the future children may use hand held devices such as iPads and tablets to support their learning. Such devices will be connected to the internet but subject to the schools filtering system. Full guidance should be drawn up in a HHD policy prior to such devices being used in school. For example, if a pupil needs to contact his/her parents/carers they should use a school phone, parents should be advised not to contact their child via their HHD during the school day, but to contact the school office.

5. Communication Policy

How will the policy be introduced to pupils?

All children in Upper School and Y2 will sign an Acceptable Use Policy agreement at the start of each academic year after the rules and procedures have been discussed in their e-safety lessons. Reference to the e-Safety policy that affects the pupils will be made at this time. Copies of these signed agreements should be taken home to be discussed with their parents and a copy returned to school for safe keeping. Children in YR to Y1 will discuss the rules as a class and then sign as a class. This document should be displayed somewhere in their class for the duration of the year.

How will the policy be discussed with staff?

This e-Safety policy has been drawn up in consultation with staff and Acceptable Use Policies were implemented as part of this process. All staff have signed the Acceptable Use Policy discussed and new staff are asked to sign the AUP upon joining the school. The signed copies are kept with the Head of CPD. The AUP is revised in line with new safeguarding legislation and

updated accordingly. Staff are aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. Staff are aware that Internet traffic can be monitored and traced to the individual user.

The school will look to implement Supply teachers being asked to sign the AUP agreement before teaching in the school and will not be asked to take charge of an Internet activity without preparation.

All school laptops and devices issued to staff by the school are covered by this e-safety policy and should not be used by third parties. Staff know of their responsibility to maintain confidentiality of school information.

How will parents' support be enlisted?
Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website. They will be invited to attend an e-Safety workshop run by an external company. Parents will be requested to read the school Acceptable Use Policy for pupils and discuss its implications with their children at the start of each academic year.

Last reviewed: September 2017
Author: Sarah Mackenzie, Head of Computing
Next review: September 2018