Park House School E-Safety Policy

1. Introduction

Students interact with the Internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger. This document, in conjunction with other Park House School Policy documents, is designed to address current issues presented as outlined below

1.1 E-Safety

E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children.

1.2 E-Safety Policy Provision

Park House School's Internet Policy will be renamed as the Park House School's E-Safety policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

Much of the material on the Internet is published for an adult audience and some is unsuitable for students. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Students must also learn that publishing personal information could compromise their security.
The school needs to protect students and staff but also to protect the School from legal challenge. The law is catching up with Internet developments: it is an offence to store images showing child abuse and to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Park House will help protect the school by making it clear to students, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised".

1.3 Statement of authority

This document has been written by teaching staff, support staff and with student input to reflect effective practice, to raise issues and to point to sources of expert knowledge. The contents have been discussed with West Berkshire Council, Park

House Staff, under previous Becta Guidelines and reference to the Child Exploitation and Online Protection centre (CEOP).
Through this Policy, Park House School is making a strong statement as to the precautions that it will take. By complying with this Policy, the school will more easily be able to demonstrate that it has taken reasonable steps to protect their students, should a serious problem arise.

1.4 School staff

IT applications are developing rapidly and can leave staff unsure of their use or how to react when students discuss their Internet use. Advice and training may be obtained from the ICT Co-ordinator or West Berkshire School's Improvement Advisor for ICT.
The trust between students and school staff is essential to education but occasionally breaks down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. The Child Exploitation and Online Protection centre (CEOP) has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders".
In industry and indeed at Park House, a member of staff who flouts IT security advice, or uses email or the Web for inappropriate reasons risks dismissal.
All staff should sign an Acceptable ICT Use Policy (AUP) on appointment. Staff accept that the school can monitor network and Internet use to help ensure staff and student safety.
Any allegation of inappropriate behaviour must be reported to the ICT Co-ordinator.
Email, text messaging and social media all provide additional channels of communication between staff and students and inappropriate behaviour can occur.
Staff and students should realise the power of the technology in Police hands to identify the sender of inappropriate messages. Park House provides the use of school owned phones for staff-student contact to ensure monitoring to protect staff from false accusations.

1.5 Routes to e-safety

The safe and effective use of the Internet is an essential life-skill, required by all students and staff. Unmediated Internet access brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations.

The e-Safety Policy will work in conjunction with other policies including Student Behaviour, Anti-Bullying and Curriculum.

1.6 Guided educational use

Curriculum Internet use produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and

educational within a regulated and managed environment in order to enrich and extend learning activities. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth. Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

1.7 Assessment of risk

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At an appropriate age they will need to learn to recognise and avoid these risks – to become "Internet Wise".
Students need to know how to cope if they come across inappropriate material.
E-Safety depends on staff, schools, governors, advisers, parents and - where appropriate - the students themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully.

Regulation
The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within the school must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access help students make responsible decisions.

1.8 Principles of Management

The school keeps an up-to-date record of access levels granted to all network users. Users are required to accept an online Acceptable Use Policy on first log-on, and for any subsequent changes. Failure to accept results in an automatic log off and a note recording this is added to the individual's file.
Senior staff, through the ICT Co-ordinator take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues by using the following appropriate strategies:
This strategy is based on limiting access, developing responsibility and on guiding students towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant. The school will take all reasonable precautions to ensure that users access only appropriate material. Filtering strategies have been selected by the school, in discussion with West Berkshire LA and the filtering provider, Openhive. The filtering strategy will be matched to the age and curriculum requirements of the Student.
However, due to the international scale and linked nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer. The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration

systems. Internet access is an entitlement for students who show a responsible and mature approach to its use. The school has a duty to provide students with safe and secure Internet access as part of their learning experience. The school Internet access is designed expressly for Staff and student use and will include filtering appropriate to the age of the student. Students are taught what is acceptable and what is not and given clear objectives for Internet use. The school ensures that the use of internet derived materials by staff and by students complies with copyright law, students are made aware of plagiarism and issues relating to research being undertaken for coursework. Staff and students are trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Staff and students need to understand that the use of the school's network is a privilege which can be removed should reason arise. The school will monitor all network and Internet use in order to ensure staff and student safety. Current methods include the use of Securus, RM Network Management tools, such as RM Tutor for live monitoring and RM Auditor for audit trails
All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

- Be polite.
- Use appropriate language.
- Do not get abusive in your messages to others.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Illegal activities are strictly forbidden.
- Note that e-mail is not guaranteed to be private.
- System administrators have access to all mail.
- Messages relating to or in support of illegal activities may be reported to the authorities.

New technologies are examined for educational benefit before use in school is allowed. Park House is currently at the forefront of the use of a huge range of new technologies and learning opportunities including:
Mobile phones with the power of a PC, with Internet, Bluetooth and wireless connectivity.
New learning environments such as Frog and other Government approved learning platforms
Thinking skills as challenged by games environments and simulations
Internet voice and messaging such as Skype and IWB linking.
Digital story telling involving independence of thought and self-motivation
Podcasting, broadcasting and recording lessons, pervasive digital video

Some of these technologies may disappear, but some will change our world. What is important is to combine the experimental ability of youth with the wisdom of teachers to develop appropriate, effective and safe uses in teaching and learning.

1.9 Response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.
The e-Safety Policy recognises the need to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.
These risks to e-safety are caused by people acting inappropriately or even illegally.
Any potential issue will be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents. All incidents relating to E-Safety reported incidents will be centrally logged on the Behaviour Management area of SIMS
This section will help staff determine what action they can take and when to report an incident of concern to the ICT Co-ordinator.
Electronic communication includes:
• Internet collaboration tools: social networking sites and blogs
• Internet research: web sites, search engines and Web browsers
• Mobile phones and personal digital assistants (PDAs)
• Internet communications: e-Mail and instant messaging (IM)
• Webcams and videoconferencing
• Wireless games consoles

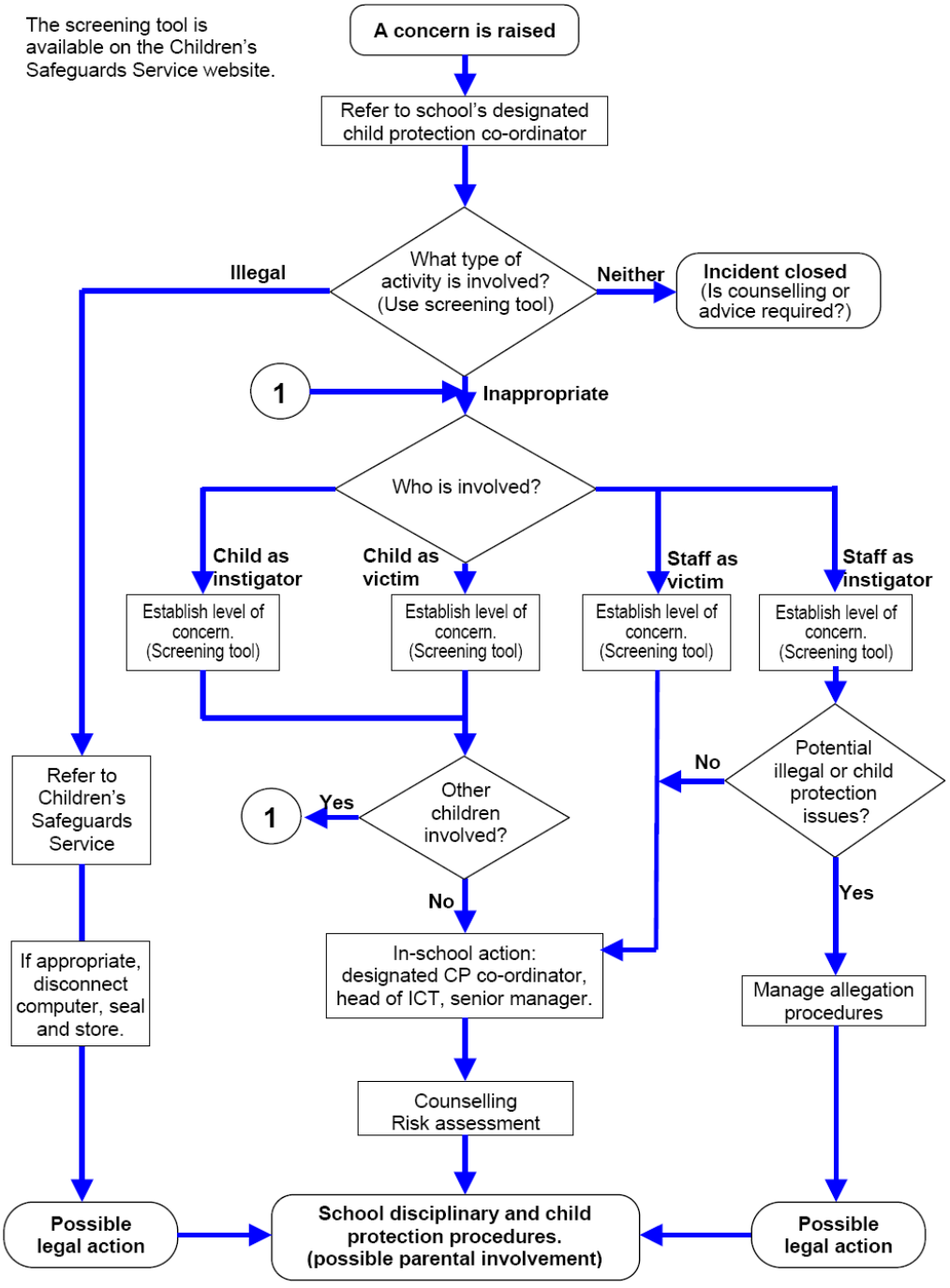
Perceived risks include:

• Receiving inappropriate content
• Predation and grooming
• Requests for personal information
• Viewing 'incitement' sites
• Bullying
• Publishing inappropriate material
• Online gambling
• Misuse of computer systems
• Publishing personal information
• Hacking and security breach

The following flowchart illustrates the approach to investigating an incident of concern

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.



2. School Responsibilities

As e-Safety has a wider responsibility than Internet use, a summary of the schools e-safety responsibilities will be included. This assists the school in developing a co-ordinated and effective approach to managing e-safety issues.

2.1 Reviewing and revising e-policy

• As Government recommends, the school has a member of staff responsible for dealing with any e-Safety issues that arise. At Park House, this is the ICT Co-ordinator in conjunction with SLT. The ICT Co-ordinator receives support and advice from West Berkshire's e-Safety Officer and where necessary, the Police.
• The ICT Co-ordinator is involved in maintaining the e-safety policy, will manage e-Safety training and keeps abreast of local & national e-safety awareness campaigns.
• The school will review their policy regularly and revise their policy annually to ensure that it is current and includes any emerging technologies used in school.
The school audits their filtering systems regularly to ensure that inappropriate websites are blocked and that students and Staff remain secure. It will also investigate any incidents of misuse.
All staff must read and sign the AUP.
• All staff, governors and parents will have access to a copy of the policy to read and review.
Implementation and Compliance
No policy can protect students by itself. Staff vigilance in planning and supervising appropriate and educational ICT experiences remains essential.

The e-safety Policy is part of the ICT Policy and School Development Plan. It relates to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship
• Our e-Safety Policy has been written by the school, building on the West Berkshire e-safety Policy and government guidance.
• The e-Safety Policy will be reviewed annually.

2.2 Teaching and E-Learning

Education develops and responds to society and the Internet and individual communications are having many effects, some profound, on society.
Less than ten years ago, we were asking whether the Internet should be used in all schools. Now every student is younger than the Internet and the World Wide Web and many use it more than their teachers. Nevertheless it is important to state what we are trying to achieve in education through ICT and Internet use.

2.2.2 Benefits to Education

• The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

• Internet use is part of the statutory curriculum and a necessary tool for learning.
• Internet access is an entitlement for students who show a responsible and mature approach to its use.
• 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.
• Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2.3 Enhancing Learning

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet in education.
Benefits of using the Internet in education include:
• access to world-wide educational resources including museums and art galleries;
• inclusion in the National Education Network which connects all UK schools;
• educational and cultural exchanges between students world-wide;
• vocational, social and leisure use in libraries, clubs and at home;
• access to experts in many fields for students and staff;
• professional development for staff through access to national developments, educational materials and effective curriculum practice;
• collaboration across support services and professional associations;
• improved access to technical support including remote management of networks and automatic system updates;
• exchange of curriculum and administration data with the LA and DCFS; access to learning wherever and whenever convenient.
Increased computer numbers or improved Internet access may be provided but effective use and quality of learning must also be addressed.
Developing effective practice in Internet use for teaching and learning is essential.
Often the quantity of information is overwhelming and staff may guide students to appropriate Web sites, or develop location skills.
The school Internet access will be designed to include filtering appropriate to the age of students.
Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students. Staff should guide students in on-line activities that will provide clear outcomes planned for the students' age and maturity.
Students will be educated in the effective use of the Internet in researching their work.

2.2.4 Content Evaluation

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. The spreading of malicious rumour has occurred for thousands of years and lies can win over truth. Information received via the Web, e-mail or text message requires superlative information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or

difficult to read. In a perfect world, inappropriate material would not be visible to students using the Web but this is not easy to achieve and cannot be guaranteed. It is a sad fact that students may occasionally be confronted with inappropriate material, despite all attempts at filtering. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
More often, students will be judging reasonable material but will need to select relevant sections. Students are taught research techniques including the use of subject catalogues and search engines and are encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Students compare Web material with other sources. Effective guided use also reduces the opportunity students have for exploring unsavoury areas.
Respect for copyright and intellectual property rights, and the correct usage of published material is taught. Methods to detect plagiarism are further developed and are certainly part of examination boards' thinking.
If staff or students discover unsuitable sites, the URL (address), is reported to the ICT Co-ordinator. School ensures that the use of Internet derived materials by staff and by students complies with copyright law.
• Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
• Students are to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
• The evaluation of on-line materials is a part of every subject.

2.3. Managing Information Services

2.3.1 Security of Information Systems

ICT security is a complex matter. A number of agencies advise on security including DCFS, West Berkshire and suppliers.
Local Area Network security issues include:
Point of Least Access
• Users must act reasonably – the downloading of large files during the working day will affect the service that others receive.
• Users must take responsibility for network use. For Park House Staff, knowingly disregarding ICT usage policy may be regarded as a matter for dismissal.
• Servers are located securely and physical access restricted.
• The server operating system is secure and kept up to date.
• Virus protection for the whole network is installed and current.
• Access by wireless devices is pro-actively managed.
Wide Area Network (WAN) security issues include:
• All Internet connections must be achieved via the West Berkshire network to ensure compliance with the security policy.
• West Berkshire firewalls and switches are configured to prevent unauthorised access between schools.
• Decisions on WAN security are made on a partnership basis between school and West Berkshire

The security of the school information systems will be regularly monitored
Virus protection will be installed and updated regularly
Security strategies will be discussed with the LA.
• Personal data sent over the Internet will be encrypted or otherwise secured.
• Files held on the school's network will be regularly checked.

2.3.2 Management of e-mail

In the school context, e-mail is not to be considered private and Park House reserves the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by legislation.
Many teenagers have their own e-mail accounts, such as the web-based Gmail, Hotmail etc. which they use widely outside school. The school bans student access to external web-based email, particularly as anonymous identities such as pjb354@mailhost.com make monitoring difficult. Strategies include limiting students to e-mail accounts on the school domain or restricting e-mail traffic to the school domain.
Much e-mail use is purely of a social nature. Spam, phishing and virus attachments can make email dangerous. Students may only use approved e-mail accounts on the school system. Students should immediately tell a teacher if they receive offensive e-mail. Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
• Access in school to external personal e-mail accounts is blocked.
• Excessive social e-mail use can interfere with learning and may be restricted.
• The forwarding of chain letters is not permitted.

2.3.3 Managing published content

The school has created excellent content on the Learning Platform that helps inspire students to publish work of a high standard. It celebrates students' work, promotes the school and has published resources for projects or homework. Editorial guidance ensures that the Web presence reflects the school's ethos that information is accurate, the site is well presented and that personal security is not compromised. Common values and quality control are shared between Web and paper publication.
Information about schools and students could be found from a newsletter but a school's
Web presence can be accessed by anyone. Publication of information is considered from a security viewpoint. Material such as staff details or a detailed plan of the school are published on the school's intranet and thereby restricted to known persons. Secure access to parts of a school web presence is for authorised people such as Governors, and is an important development.
The contact details on the Web site are the school address, generic e-mail and telephone number. Staff or students personal information will not be published.
• Email addresses are published carefully, to avoid spam harvesting.
• The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

• The Web presence complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Publication of student's images or work

Photographs that include students add a liveliness and interest to a Web presence or blog that is difficult to achieve in any other way. Nevertheless the security of staff and students must come first. Although common in newspapers, the publishing of students' names with their photographs is not acceptable. Web images could be misused and individual students identified unless broad descriptions are used.
Strategies include using relatively small photographs of groups of students and using photographs that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational activity and personal photographs can be replaced with self-portraits or images of students' work or of an activity.
Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
Students' full names will not be used anywhere on the Web area, particularly in association with photographs.
• Student's work can only be published with the permission of the student and parents.

2.3.5 Managing social networking and personal publishing

Teachers are aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Students are encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.
Examples include: blogs, wikis, Facebook, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.
The School blocks/filters access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.
Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
• Students are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
• Teachers' official blogs or wikis are password protected and run from the school Learning Platform. Teachers are advised not to run social network spaces for students on a personal basis.

• Students are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.
• Students are advised not to publish specific and detailed private thoughts.
• School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

2.3.6 Managing filtering

Internet access is made appropriate for all members of the school community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use is recognised and restrictions may be removed temporarily. Systems to adapt the access profile to the student's age and maturity will become available.
The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):
• Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
• A walled-garden or allow list provides access only to a list of approved sites.
Such lists inevitably restrict students' access to a narrow range of information.
• Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Outgoing information such as Web searches is also filtered.
• Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
• Access monitoring records the Internet sites visited by individual users. Access to a site forbidden by the filtering policy is monitored.
Hundreds of inappropriate sites are created each day and many change URLs to confuse filtering systems. Management time will be considerable.
The school works in partnership with West Berkshire and the Internet Service Provider to ensure filtering systems are as effective as possible.
If staff or students discover unsuitable sites, the URL and/or other content is reported to the ICT Co-ordinator.
• The school manages the configuration of their filtering. This task requires both educational and technical experience.
• Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
Any material that the school believes is illegal is reported to external agencies
Filtering strategies are selected by the school, in discussion with the filtering provider where appropriate.

2.3.7 Managing videoconferencing

Since the National Educational Network (NEN) has been developed, under the Government's 'Harnessing Technology' directive, it provides a secure, broadband, IP network interconnecting the ten regional schools networks across England with the Welsh, Scottish and the Northern Irish networks.
Park House can thus use IP technology in a secure and managed environment.
The school has full 'DfE Specification' broadband are connected through the LA and Regional Broadband Consortia and have access to services such as gatekeepers and gateways to enable schools to communicate with other locations outside West Berkshire. MCUs (Multipoint Control Units) enable several schools to communicate at one time, for instance with several video streams each in a screen window.
The equipment and network
IP videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
Equipment connected to the educational broadband network uses the national E.164 numbering system and displays their H.323 ID name.
External IP addresses are not made available to other sites.
• Videoconferencing contact information will not be put on the school web area.
• The equipment will be secure and if necessary locked away when not in use.
• School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users
Students should ask permission from the supervising teacher before making or answering a videoconference call.
Videoconferencing should be supervised appropriately for the students' age.
• Parents and Guardians should agree for their children to take part in videoconferences, in the annual return.
• Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
• Only key administrators have access to the videoconferencing system web or other remote control page available on larger systems.
• Unique log on and password details for the educational videoconferencing services are only issued to members of staff and kept secure.
Content
When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
Recorded material shall be stored securely.
If third-party materials are to be included, it is necessary to check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).

2.3.8 Managing emerging technologies

E-mail can be sufficient to set up a virtual community. The students in two schools could create a shared project using class e-mail and a common Web site or blog. Staff and Governors make a larger community, which should be extended to include parents. Virtual classrooms and virtual communities widen the geographical boundaries of learning. New approaches such as mentoring and parent access to assessment scores now form part of Government 'Every Child Matters 'initiative. Is an on-line community one way to encourage a disaffected student to keep in touch?
The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school is difficult as demonstrated by social networking sites such as Twitter and Facebook. The registering of individuals to establish and maintain validated electronic identities is an important part of the process.
Video conferencing introduces new dimensions. Web cameras cost as little as £10 and, with faster Internet access, can enable limited video to be exchanged across the Internet. The availability of live video can impact on safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details.
New applications are continually being developed based on the Internet, the mobile phone network, wireless or infrared connections. Users can be mobile using a phone or personal digital assistant with wireless Internet access.
Schools should keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many students. Could teachers communicate with a truanting student? Could reminders for exam coursework be sent by text message? There are dangers for staff if personal phones are used to contact students and a school owned phone will be issued.
The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Students need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages is dealt with under the school bullying policy.
• Emerging technologies will be examined for educational benefit before use in school is allowed.
• Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
• The school should investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use in school.
• Staff will be issued with a school phone where contact with students is required.

2.3.9 Protecting Personal data

The quantity and variety of data held on students, families and on staff is continually expanding. While this data can be very useful in improving services, data can be mishandled, stolen or misused.
The Freedom of Information Act gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information

is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual). The act also gives rights to the people the information is about i.e. the right of subject access, lets individuals find out what information is held about them.
The eight principles are that personal data must be:
• Processed fairly and lawfully
• Processed for specified purposes
• Adequate, relevant and not excessive
• Accurate and up-to-date
• Held no longer than is necessary
• Processed in line with individuals rights
• Kept secure
• Transferred only to other countries with suitable security measures.
Park House already has information about their obligations under the Act, and this section is a reminder that all data in which people can be identified is protected.
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 Authorisation of Internet Access

The school allocates Internet access for staff and students on the basis of educational need. Authorisation is on an individual basis. As most students will be granted Internet access, a list of those denied access is posted in the Staff shared area of the school network. Parental permission is required in all cases and is addressed on student entry to school.
The school maintains a current record of all staff and students who are granted Internet access.
All staff must read and sign the 'Acceptable ICT Use Policy' (AUP) before using any school ICT resource.
• Parents are asked to sign and return a consent form for student access.
Assessing risk
As the quantity and breadth of the information available through the
Internet continues to grow it is not possible to guard against every undesirable situation.
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school

computer. Neither the school nor West Berkshire LA can accept liability for the material accessed, or any consequences of Internet access.
• The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
• Methods to identify, assess and minimise risks will be reviewed regularly.
The head teacher through the ICT Co-ordinator will ensure that the e-compliance with the policy is monitored.

2.4.2 Handling reported E-safety incidents

Parents, teachers and students should know how to submit a complaint.
Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.
A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions are in place, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e-Safety coordinator.
See also section 1.9 Response to an incident of concern.
Complaints of Internet misuse will be dealt with in the first instance, by with the ICT Co-ordinator.
Any complaint about staff misuse must be referred to the head teacher.
• Students and parents will be informed of the complaints procedure.
• Parents and students will need to work in partnership with staff to resolve issues.
• Discussions will be held with the local Police Youth Crime Reduction Officer liaison officer to establish procedures for handling potentially illegal issues.
• Sanctions within the school Behaviour Policy include:
– interview/counselling by head of year;
– informing parents or carers;
- removal of Internet or computer access for a period.
Whilst each case is judged on its' merits, general rule of thumb is as follows:

Unauthorised access to the internet and/ or accessing inappropriate material 2 week internet ban
Actively breaching school internet security to access otherwise banned sites, i.e. use of proxy servers 4 week internet ban
Sending offensive email through the Park House web based mail system, 2 week email ban (depending on severity)
Wilful damage of Park House computing facilities, ban on use determined by severity

2.4.3 Community Internet use

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is developing access appropriate to its own client groups and students may find

variations in the rules and even unrestricted Internet access. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content, copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with students on the reasons for the differences could be worthwhile.
Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the students' cultural backgrounds.
• The school will liaise with local organisations to establish a common approach to e-safety.
• The school will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

2.5 Communications Policy

2.5.1 Introducing policy to students

Many students are very familiar with Internet use. As students' perceptions of the risks will vary, the rules for responsible use may need explanation and discussion. Students are reminded of the school rules, by posters at the point of Internet use.
Consideration is given as to the curriculum place for e-safety, is it an ICT activity, part of the pastoral programme or part of every subject?
Rules for Internet access will be posted in all networked rooms.
Students are informed that Internet use will be monitored.
• Instruction in responsible and safe use precedes Internet access.
• A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

2.5.2 Introducing policy to staff

The School e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies.
Staff must understand that the Internet misuse rules for Park House employees are quite specific. Instances of misuse resulting in dismissal have occurred. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with their line manager or ICT Co-ordinator to avoid any possible misunderstanding.
Internet use is widespread and all staff including administration, caretaker and governors are included in appropriate awareness raising and training. The induction of new staff discusses Internet issues.

All staff will have access to the School e-Safety Policy and its importance explained.
• Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

• Staff that manage filtering systems or monitor ICT use will be supervised by the ICT Co-ordinator and senior management and have clear procedures for reporting issues.
• Staff development in safe and responsible Internet use and on the school e-Safety Policy is provided as required.

2.5.3 Parental Support

Internet use in students' homes is now the norm, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, students may have unrestricted access to the Internet.
Parents should also be advised to check if students' use elsewhere is covered by an appropriate use policy.
• Internet issues will be handled sensitively to inform parents without alarm.
• Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is made available to parents on request.

3. Legal Framework

An awareness of legal issues is important.
Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes include:
• The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.
• Offences regarding racial hatred are covered by the Public Order Act 1986 and the Racial and religious Hatred Bill 2005.

3.1 Possible offences:

Sexual Offences Act 2003
• Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
• Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)
• Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
• Abuse of positions of trust - Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under
18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, connexions staff)
N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs.

3.2 Relevant Legislation

The Computer Misuse Act 1990 - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.
Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.
Communications Act 2003 - There are 2 separate offences under this act: a. sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. b. sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

This wording is important because the offence under a. is complete when the message has been sent - no need to prove any intent under b. to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.
Malicious Communications Act 1988 – offence to send a letter, e-communication or article which is indecent or grossly offensive, threatening or finding information with intent to cause distress or anxiety to the recipient.
Copyright, Design and Patents Act 1988 - it is an offence to use unlicensed software
Protection of Children Act 1978 - The law on images covers the offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.
Obscene Publications Act 1959.
Protection from Harassment Act 1997
Section 2 - A person must not pursue a course of conduct—
(a) which amounts to harassment of another, and
(b) which he knows or ought to know amounts to harassment of the other.
Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
.
3.3 Monitoring

Monitoring School ICT use network activity could contravene Article 8 of the Eu Monitoring Human Rights and Fundamental Freedoms, e.g. the right to respect for private family life, which is protected by the Human Rights Act 1998.
The Telecommunications (Lawful Practice) (Interception of Communications)
Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitors information generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection ofrights and freedoms of others. Park House ensures that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

3.4 Sex Offences Act 2003 Memorandum of Understanding

Memorandum of Understanding between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum was created within the context of child protection, which will always take primacy.

E-Saftey Delivery for Students, Staff and Parents of Park House School

In line with current OfSted requirements and to ensure the welfare of all staff, students and parents of Park House School we intend to deliver the following programmes on an annual basis:

Staff:	Time of Year
An induction from Sharon Upton on E-Safety when joining the school with a signed declaration at the end. This will be updated annually at September inset;	September/start of term as appropriate
A termly focus in department meetings on current E-Safety issues facing students/staff/PHS;	September/January/May
An e-safety policy which clearly states the process for dealing with common issues staff may encounter professionally;	September and updated annually
Prompts for password changes every term;	Termly
Encryption of (portable data devices) or encrypted remote (access) WAN, currently out to tender;	As of June 2015
An online e-safety questionnaire to assess staff views and capability.	April INSET
Parents:	**Time of Year**
An annual e-safety letter sent home with tips for parents;	September with curriculum information
An online e-safety questionnaire to assess parental views and inform subsequent information sent home;	September with curriculum information
E-safety guidance provided at years 7-11 parent evenings, this opportunity could also be used for governor's to attain some feedback on the evening.	At parent evenings
Students:	**Time of Year**
The school website/students' desktops to have a permanent link to either the smile email account of the CEOP;	Ongoing
The school council to have annual input into the e-safety policy of the school;	June/July
A DfE approved Educational web filtering system in place to filter web content;	Ongoing
An online e-safety questionnaire to assess student views, inform subsequent information provided and assess any areas that are causing concern;	June/July
Some aspects of e-safety delivered through the computing curriculum, others through a tutor programme that is differentiated by year group from years 7-10 as shown in the table below;	Ongoing
Annual Safer Internet Day/Week delivery of assemblies and other assorted activities.	February

Area	Year Group	Delivery
Grooming	7	Tutor/PDP
Cyber-bullying in all forms	7	Tutor/PDP
Identity theft (including 'frape') and sharing passwords	7	Tutor/PDP
Privacy issues, including disclosure of personal information	8	Tutor/PDP
Digital footprint and online reputation	8	Tutor/PDP
Exposure to inappropriate content, including online pornograpy; ignoring age ratings in games (exposure to violence, often associate with racist language); substance abuse and 'revenge porn'	9	Tutor/PDP
Health and well-being (amont of time spent online gaming/internet)	9	Tutor/PDP
Sexting also referred to as SGII	9	Tutor/PDP
Lifestyle websites, for example pro-anorexia, self-harm or suicide sites	10	Tutor/PDP
Hate sites	10	Tutor/PDP
Content validation: how to check authenticity and accuracy of online content	7 and 8	Curriculum
Copyright (little care or consideration for intellectual property and ownership such as music and film)	Throughout the curriculum	Curriculum