Parkgate House School

E-Safety Policy

PARKGATE HOUSE SCHOOL E-SAFETY POLICY

This policy has been written in consultation with staff and the senior management team of Parkgate House School. This policy has been developed as a result of a process of consultation . It has been agreed by senior managers and approved by the Designated Person responsible for Safeguarding and Child Protection. It builds on Becta guidance and the exemplar policy of the London Grid for Learning (LGfL). It is a statement of the aims, principles and strategies for the safe use of Internet and related technologies at Parkgate House School.

Philosophy

"Everyone has a role to play in empowering children to stay safe while they enjoy the new technologies, just as it is everyone's responsibility to keep children safe in the nondigital
world." Byron Report – Safer Children in a Digital World. (March 2008)

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Aims

The philosophy of 'empowering children to stay safe' includes aims that children are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- An e-Safety education programme for pupils, staff and parents.

(Reference: Becta - E-safety Developing whole-school policies to support effective practice 1)

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of the senior management team, aims to embed safe practices into the culture of the school. The Principal ensures that the Policy is implemented and compliance with the Policy monitored.

The responsibility for e-Safety has been designated to Miss Catherine Shanley, Principal.
Our school e-Safety Co-ordinator is, Mr. Malcolm McKinlay, Deputy Headmaster
Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through organisations such as DFE and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator also ensures the Principal and senior management team are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Accessing the Internet
The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read and sign the Staff Code of Conduct for Acceptable Internet Use before using the school ICT resource.
For younger children (Nursery and Reception), access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on –line materials. Pupils from PP1 (year 1) to Prep 6 (year 6) will be given supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form for pupil access. Parents will be informed that pupils will be provided with supervised Internet access.

The Internet and Learning
Effective practice in Internet use for teaching and learning is essential as the quantity of information can be over whelming . Younger children should be offered selected sites rather than the open Internet search. Older children benefit from the same use of suggested sites and must also be encouraged to evaluate everything they read and to refine their own publishing.
Plagiarism will be discouraged at all times and children will be taught to acknowledge sources in their work. The school internet access will be designed expressly for pupil use and will include filtering appropriate to primary school children. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

At present, these rules are based on Childnet's SMART rules for children and are displayed in PP1-P6 classrooms :

S – Stay safe, do not give out personal information
M – Tell an adult if you are thinking of meeting someone.
A – Accepting e-mails or open attachments from people you do not know can lead to viruses and unwanted emails.
R – Information you find on the Internet may not be reliable and people may not be who they say they are.
T– Tell a parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried, and if you or someone you know is being bullied online.

Other teaching tools include the use of e-safety websites including:
Think U Know (www.thinkuknow.co.uk)
Grid Club (www.gridclub.com)
Kidsmart (www.kidsmart.org.uk)
Bizzikid (www.bizzikid.co.uk)

E-mail

Parkgate House School provides pupils with the opportunity to use email in a safe, approved email environment.

Website

Contact details on the website will include school address, e-mail and telephone number. Staff or pupils' personal details must not be published. No link should be made between an individual and any home address (including simply street names);

The Principal will take overall editorial responsibility to ensure that content is accurate and appropriate. The school must respect intellectual property rights and copyright.

The publishing of pupils' names with their images is not acceptable. Images should be carefully chosen so that individuals can not be identified.

Written permission will be sought from parents before publication of any images on the web site or newsletter.

Work can only be published with the permission of pupil and parents.

Social Networking

Examples of social networking sites include- wikis, blogs, MySpace, MSN space, bulletin boards, chat rooms, instant messaging and many others. As children can access these at home, advice to children will be supplemented by similar advice to their parents. The School will block access to these social networking sites and others.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Pupils will be advised not to place personal photos on any social network space. Staff are also encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

It is recognised that some such services may have an appropriate application in school, however, where such activities are planned a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by a member of the Senior management team prior to use.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Managing Filtering

At present, Parkgate House School uses 'The Sonicwall Content Filtering System', a dynamic service which filters Internet sites and the school also endeavours to block unsuitable sites as reported.

To this end we will:-

Work with our Internet Service Provider (Easynet) to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported immediately to the

e-Safety Coordinator.
Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Mobile Phones and Hand-held Devices
Mobile phones should not be used by pupils in school time. The sending of abusive or inappropriate text messages is strictly forbidden.

Use of Portable Equipment
The school provides ICT equipment such as computers, Ipads, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities. Exactly the same principles of acceptable use apply as in other sections of this policy:

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the ICT co-ordinator;

- Certain equipment will remain in the care of the ICT co-ordinator, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the IT Office;

- Equipment such as laptop computers and Ipads can be taken offsite for use by staff in accordance with the E-Safety Policy and the equipment is fully insured from the moment it leaves the school premises. The cover excludes theft or attempted theft from an unattended vehicle unless the vehicle is locked, there are signs of forced entry and the property is out of sight in a locked compartment or boot within the vehicle.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;
- If an individual leaves the employment of the school, any equipment must be returned;

- The use of USB pens, re-writeable CDs, floppy disks etc. must be regulated . Where information has been downloaded from the internet, or copied from another computer, wherever possible, it must be emailed to school to ensure that it undergoes anti-virus scanning. If this proves to be impossible, (due to file size, technical difficulty etc.) express permission must be sought from the ICT coordinator prior to the data being transferred;

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software.

Roles and Responsibilities

Responding to an incident of concern
Our e-Safety Coordinator acts as first point of contact for any complaint.
Complaints of Internet misuse will be dealt with by a senior member of staff.

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

1. Pupils should notify a teacher immediately.
2. The e-Safety Coordinator should be notified and the incident reported to the Principal.
3. The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party.
4. The child's parents should be notified at the discretion of the Principal according to the degree of seriousness of the incident.

Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a disciplinary matter and the parents of the child or children will normally be informed. If deliberate access to undesirable materials is found to be repeated, flagrant or habitual the matter will be treated as a serious disciplinary issue. The child or children's parents will be informed and the Governing body advised.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:

- interview/counselling Principal/e-Safety Coordinator;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system;
- Referral to police.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
Complaints related to child protection are dealt with in accordance with school child protection procedures.

Staff

All staff will be given the School e-Safety Policy and its application and importance explained. Staff are required to read and sign a ‘Code of Conduct’ regarding Acceptable Use of the school’s information system. (**See Appendix ICT:1**). Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The ICT Technician (Cardonet Representative), who at present manages the filtering systems, will be supervised by senior management and have clear procedures for reporting issues.
Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required, and formally every two years. Any complaint about staff misuse must be referred to the Principal.

All Staff Training received: 2/9/11 E-Safety for Teachers Staff Training w/ Mary Rebelo (Accredited CEOP Child Exploitation and Online Protection Agency ambassador)
Re: Intro to Internet Safety, cyberbullying and risks.

Parents
Parents' attention will be drawn to the school's e-Safety Policy in newsletters, and on the school website. Parents of pupils entering PP1 (or any pupils joining a year group above PP1) are required to read and agree to the school's Statement of Acceptable Use for ICT. A partnership approach with parents will be encouraged.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. (see list of e-safety sites above)

Specific Learning Needs
Provision for children with specific learning needs in relation to e-Safety is made after discussion between class /subject teacher, support staff and the SENCO.
Some groups of children are potentially more vulnerable and more at risk than others when using ICT. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children.

Children with Specific Learning Needs can use the internet in educational, creative, empowering and fun ways, just like their peers. However, they may be particularly vulnerable to e-safety risks. For example:

- Children and young people with Autism Spectrum Disorder may make literal interpretations of content, which will affect how they respond;
- Some children may not understand much of the terminology due to language delays or disorders;
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet;
- There is also growing concern around cyberbullying. We need to remember that some children with Specific Learning Needs or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied;
- In addition, some children may not appreciate how their own online behaviour

may be seen by someone else as bullying.

Where appropriate, special adaptations, such as video presentations with signing and the use of Widgit cards for poorer readers, of Childnet International’s SMART resources can be accessed. Teachers should tackle these sensitive issues sympathetically. The SENCO should ensure that strategies for safe internet use are part of individual children's learning plan.

E-Safety Curriculum

E-Safety for the Early Years and Foundation Stage

In the Early Years and Foundation Stage children experience the Internet with close adult supervision to play games and look at pictures. They use simulations of activities and situations and talk about what is real and what is imaginary. They learn to ask an adult for support straight away if they come across anything on the Internet they think is unsuitable or that distresses them. They begin to use communication tools under close adult supervision and with adult assistance and learn about different ways of communicating with others. They use “technology” in role play, learning about the place of technology in the World and some of the safety risks associated with technology. They help each other in their use of technology, taking turns and sharing.

	Knowledge and understanding	**Skills**	**Responsibilities**	**Some suggested activities**
EYFS	Children should be able to: • Identify people who can help when using ICT and seek their help when appropriate. • Understand that ICT can be used for fun, for learning and for communicating with others. • Understand that some technologies should only be used when adults are present. • Understand that the school Extranet/learning platform is a safe place to share pictures and messages but that other places may not be safe. • Understand that they can use technology to share information.	Children should be able to: • Recognise the difference between real and imaginary experiences. • Recognise that some choices might be right and others wrong. • With support, use simple passwords to access ICT.	Children should: • Share equipment and take turns. • Follow school and family guidelines that promote responsible use of ICT.	Teachers provide opportunities for children to: • Share learning with families online. • Set ICT toys for indoor and outdoor play that mimic technology in real life. • Explore onscreen activities that mimic real life. • Talk about the differences between real and imaginary experiences. • Talk about appropriate behaviour when using various ICT equipment. • Understand who will help them if they are worried or frightened when using ICT equipment. • Use ICT equipment or networks/Extranet with adult support to send positive messages to other class members.

E-Safety for Key Stage 1

In Key Stage 1 children develop an understanding of different means of communication and learn that they must know the person they are communicating with, unless an adult has agreed the communication is safe (e.g. a request for information to a specific museum). They begin to learn about the Internet and they use websites under supervision to look for information and to play games, particularly games for learning. They know that the Internet has advertising on some websites. They use passwords to access some ICT at school and learn that they need to keep passwords private. They know that they cannot always copy things they find on the Internet because they belong to other people. They know how to act if they find an unsuitable website. They treat other people, and other people's work, with respect when working and communicating with ICT.

	Knowledge and understanding	**Skills**	**Responsibilities**	**Possible activities**
KS1	Children should be able to: • Recognise the need to know who it is they are sharing their learning with online. • Understand the different methods of communication (e.g. email, online forums). • Know the difference between email and communication systems such as blogs, discussion forums and wikis. • Know that websites sometimes include pop-ups that take them away from the main site and that these may be advertising. • Know that bookmarking is a way to find safe sites again quickly. • Begin to evaluate websites and know	Children should be able to: • Know what to do if they find something inappropriate online (including identifying people who can help) • Use the Internet for fun learning and communicating with others, supervised by a responsible adult and making choices when navigating through sites. • Send and receive email as a class or under close supervision from a responsible adult. • Recognise advertising on websites and learn to ignore it. • Use a password to access the school network	Children should: • Understand that they need to keep their passwords private, except from a trusted adult. • Respect the work of other which is stored on a shared drive of a network or presented online. • Treat people politely online.	Teachers provide opportunities for children to: • Practice minimising a screen or switching off the monitor if they encounter a problem on a website. • Use (and sometimes create) a password to access files or websites. • Talk about the importance of remembering their passwords and keeping them private. • Use online tools to work collaboratively on simple tasks with their peers. • Draw up a list of people who can be accessed for help if they access something that makes them feel uncomfortable. • Search for specific key words using a teacher-selected website or CD-ROM. • Navigate websites and discuss the content. • Send and receive emails within safe

	that not everything on the Internet is true. • Know that sometimes pictures and words on the Internet cannot be copied because they belong to somebody (copyright).	or other account.		systems.

E-Safety for Early Key Stage 2

In years 3 and 4 children develop more independence in their use of the Internet, carrying out searches for information within websites and using child-friendly search engines. They begin to assess the information they find on the Internet for its fitness for purpose and its accuracy. They discuss the use of communication tools, what it may be unsafe to reveal when using these tools and when the use of a nickname provides for greater safety online. Children's management of email is extended to develop an awareness of spam and the risks involved in opening attachments. They know that work and other material on the Internet may be copyrighted and that they should acknowledge the sources of information they use in reports or presentations. They understand that new technologies may be used inappropriately by others, including their peers, and they know what to do if this happens to them or to others.

	Knowledge and understanding	**Skills**	**Responsibilities**	**Possible activities**
Y3/4	Children should be able to: • Understand the need for rules to keep them safe when exchanging learning and ideas online. • Recognise that information on websites may not be accurate or reliable and may be used for bias manipulation or persuasion. • Understand that the Internet contains fact,	Children should be able to: • Identify risks and rewards of using the Internet and use safe practices which help maintain both personal safety and the safety of equipment. • Contribute to and use basic guidelines and practices that promote e-safety and socially healthy use of	Children should: • Respect the ideas and communications of others in work which is presented in an electronic format. • Recognise the effect their writing or images might have on others (including bullying) and act accordingly.	Teachers provide opportunities for children to: • Use the Internet for research and gather information in the form of text and images. • Discuss when the Internet is useful and when it should be used with caution. • Use online tools to collaborate and exchange information with others within and beyond their school. • Design a nickname for use online and discuss whether it is ok to share

	fiction and opinion and begin to distinguish between them. • Understand the need to keep personal information and passwords private. • Understand that if they make their personal information available online it may be seen and used by others.	ICT. • Recognise the difference between the work of others which has been copied (plagiarism) and re-structuring and re-presenting materials in ways which are new and 'unique'. • Begin to identify when emails should not be opened when an attachment may not be safe. • Understand the need to develop an alias for some public online use.		this information with classmates. • Discuss the use of communication tools e.g. forums, instant messaging, email.

E-Safety for Later Key Stage 2

In years 5 and 6 children develop a greater understanding of the potential risks involved in using on-line communication tools and they develop skills to help them manage those risks. They begin to select appropriate collaboration tools for their learning and they use the responsibly. They create and use strong passwords. They have more independence in using the Internet and begin to refine their skills of assessing information and to look at bias and commercial interests as well as accuracy. They take more responsibility for their own safety and wellbeing and that of others when using the Internet and online communications tools, recognising their own right and that of others to be treated with respect and courtesy online.

	Knowledge and understanding	**Skills**	**Responsibilities**	**Possible activities**
Y5/6	Children should be able to: • Explore and discuss both positive and negative impacts of the use of ICT in their own lives and those of their peers and family. • Understand the	Children should be able to: • Access and use information to identify e-safety risks to themselves or equipment, and make safe choices when using ICT.	Children should: • Evaluate their own use of websites and how they present themselves online. • Recognise their own right to be protected from the inappropriate use of technology by others and the need to	Teachers provide opportunities for children to: • Discuss the possible consequences of sharing personal details online and how to respond when asked for those details. • Discuss the consequences of trusting

	potential risks of providing personal information online. • Recognise reasons why people might publish content that is not accurate and understand the need for critical evaluation of websites. • Understand that some websites and/or pop-ups have commercial interests that may affect the way information is presented. • Recognise the potential risks of using Internet communication tools and understand how to minimise those risks (including scams and phishing). • Understand that some material on the Internet is copyrighted and may not be copied or downloaded.	• Research current e-safety guidelines and practices which are relevant to their own use of ICT and take action to promote e-safety to their peers and family. • Use the Internet in ways which minimise risks, e.g. responsible use of chat rooms and discussion forums, safe use of webcams. • Select an appropriate tool to undertake activities which provide opportunities to collaborate and communicate safely with others within and beyond their school. • Create strong passwords and manage them so they remain strong.	respect the rights of other users in the same way.	information and people on the Internet. • Explore issues linked to copyright and plagiarism. • Use, and begin to evaluate, online tools to exchange information and collaborate with others within and beyond the school. • Identify and evaluate differences in information from a variety of sources, considering its plausibility and developing strategies to make judgements on the sources used. • Evaluate websites and describe the possible impact of published content on an audience, e.g. the use of advertising and how sites might be designed to persuade and influence.

Equal Opportunities

All teaching and non-teaching staff at Parkgate House School are responsible for ensuring that all children, irrespective of gender, ability, ethnicity and social circumstances, have access to the whole curriculum and make the greatest possible progress. Equal access needs to be planned and monitored very carefully and this must be reflected in teacher's pairs and groupings. General monitoring is the responsibility of the Principal, the Deputy Headteacher and the e-safety co-ordinator.
Where use of a school computer proves difficult for a child because of a disability, the school will provide specialist equipment and software, so that the pupil may have access. (i.e. lower case lettering on keyboards, concept keyboards, roller ball mouse, filter screens.) Pupils with learning difficulties can also be given greater access to the issues of e-Safety through the use of I.C.T.

Review

The speed and nature of development is such that a review of the e-Safety Policy should take place on an annual basis, in the Spring Term. The e-safety Co-ordinator then makes any changes or adaptations of policy. Throughout the year, all staff are encouraged to feed back information about the effectiveness of this policy and ideas to the e-safety co-ordinator.

Wandsworth Advice

The following guidelines for managing e-safety specific incidents have been proposed by Wandsworth Council (Reference: WSCB – E-Safety Policy):

An inappropriate website is accessed unintentionally in a school or children's setting by staff or a child. 1. Play the situation down; don't make it into a drama. 2. Report to the Principal/senior manager/e-safety lead officer and decide whether to inform parents of any children who viewed the site. 3. Inform the school or organisation's technical: support and ensure the site is filtered	**An inappropriate website is accessed intentionally by a child.** 1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions. 2. Notify the parents/carer of the child. 3. Inform the organisation's technical support and ensure the site is filtered if need be.
An adult uses an organisation's ICT equipment inappropriately. 1. Ensure you have a colleague with you, do not view the misuse alone. 2. Report the misuse immediately to the Principal/ senior manager/e-safety officer and ensure that there is no further access to the PC or laptop. 3. If the material is offensive but not illegal, the Principal/senior manager/e-safety officer should then: 4. Remove the PC to a secure place. 5. Instigate an audit of all ICT equipment by the ICT technical support providers to ensure there is no risk of others accessing	**A bullying incident directed at a child occurs through email or mobile phone technology.** 1. Advise the child not to respond to the message. 2. Refer to relevant policies including e-safety anti-bullying and apply appropriate sanctions. 3. Secure and preserve any evidence. 4. Inform the sender's email service provider. 5. Notify parents/carers of the children involved. 6. Consider delivering a parent/carer workshop for the community. 7. Inform the police if necessary. 8. Inform Wandsworth's e-safety officer.

inappropriate materials. 6. Identify the precise details of the material. 7. Take appropriate disciplinary action (contact Personnel/Human Resources). 8. In an extreme case where the material is of an illegal nature: 9. Remove the PC to a secure place and document what you have done. 10.Contact the local police and follow their advice.	
Malicious or threatening comments are posted on an internet site about a child or member of staff. 1. Inform and request the comments be removed if the site is administered externally. 2. Secure and preserve any evidence. 3. Send all the evidence to CEOP at: www.ceop.gov.uk/contact_us.html 4. Endeavour to trace the origin and inform police as appropriate. 5. Inform Wandsworth's e-safety officer.	**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.** 1. Report to and discuss with the named child protection officer/lead officer for safeguarding and contact parents/carers. 2. Advise the child on how to terminate the communication and save all evidence. 3. Contact CEOP: www.ceop.gov.uk 4. Consider the involvement of police and Children's Services. 5. Inform Wandsworth's e-safety officer. Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology - they must be able to do this without fear.

E-Safety Policy Audit Summary (Proposed by Wandsworth Safeguarding Children's Board)

This quick self-audit will help senior staff assess whether the e-safety basics are in place to support a range of activities.

Has the school/setting an e-safety policy that complies with Wandsworth Children's Services e-safety guidance?	YES
Date of latest update:	March 2013
The policy was agreed on:	March 2013
The policy is available for staff at:	Shared Area / Policies and Curriculum Map Folder And on the school website.
The policy is available for parents at:	The School Office and on the school website
The Designated Child Protection Co-ordinator is:	Catherine Shanley
The e-Safety Co-ordinator is:	Malcolm McKinlay
Has e-safety training been provided for both students and staff?	Staff – Staff Induction Mtg w/ MCK and 2/9/11 all staff

	training w/ E-Safety for Teachers Staff Training w/ Mary Rebelo (Accredited CEOP Child Exploitation and Online Protection Agency ambassador) Re: Intro to Internet Safety, cyberbullying and risks. Pupils – September/October 2011 – rescheduled for Sept13
Do all staff sign an ICT Code of Conduct on appointment?	YES
Have school e-safety rules been set for students?	YES
Are these rules displayed in all rooms with computers?	YES
Do parents sign and return an agreement that their child will comply with the e-safety rules?	YES
Internet access is provided by an approved educational internet service provider and complies with DFE requirements	YES
Has an ICT security audit has been initiated by senior staff, possibly using external expertise?	YES - CARDONET
Is personal data collected, stored and used according to the principles of the Data Protection Act?	YES – See Data Protection Policy in Staff Handbook
The following bullets below are the essential minimum points for an e-Safety Policy as determined by Wandsworth Council. The listed elements enable demonstration that the e-Safety Policy is compliant with the Wandsworth Children's Services approved policy. Naturally, policy must be translated into practice to protect children and educate them in responsible ICT use.	
Writing and reviewing the e-Safety Policy	
The school will appoint an e-Safety Co-ordinator. This may be the Designated Child Protection Co-ordinator as the roles overlap.	Malcolm Mckinlay is the appointed coordinator
Internet use will enhance learning	
Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.	YES
Pupils will be taught what Internet use is acceptable and what is not and given suitable guidance.	YES
Children will be taught how to evaluate Internet content	
We will ensure that the use of internet derived materials by staff and children, complies with copyright law.	YES
Information system security	
ICT systems capacity and security will be reviewed regularly.	YES – CARDONET
Virus protection will be updated regularly.	YES – CARDONET
Security strategies will be discussed with Wandsworth Children's Services ICT support.	YES – CARDONET (IF APPROPRIATE)
Email	
Children may only use approved email accounts on the school/setting system.	YES – SmartLearning + in future possibly one other
Children must immediately tell a member of staff if they receive offensive email.	YES
Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.	YES
Published content and the school website	
The contact details on the website should be the school/setting address,	YES

email and telephone number. Staff or children's personal information will not be published.	
Publishing children's images and work	
Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.	YES
Children's full names will not be used anywhere on the website or blog, particularly in association with photographs.	YES
Written permission from parents or carers will be obtained before photographs of children are published	YES – PHOTO CONSENT FORM
Social networking and personal publishing	
The school/setting will block/filter access to social networking sites, but may allow them for specific supervised activities.	YES
Newsgroups (which are news chat rooms) will be blocked unless a specific use is approved.	YES
Children will be advised never to give out personal details of any kind which may identify them or their location.	YES
Managing filtering	
The school will work with the LA, DFE and the internet service provider to ensure systems to protect children are reviewed and improved.	YES
If staff or children discover an unsuitable site, it must be reported to the e Safety Co-ordinator.	YES
Managing video-conferencing	
IP video-conferencing should use the educational broadband network to ensure quality of service and security rather than the internet.	YES
Children should ask permission from the supervising member of staff before making or answering a video-conference call.	YES
Video-conferencing will be appropriately supervised for the children's age.	YES
Managing emerging technologies	
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in a school/setting is allowed.	YES
Protecting personal data	
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.	YES – See Data Protection Policy in Staff Handbook
Authorising internet access	
All staff must read and sign the 'Acceptable ICT Use Agreement' before using any ICT resource.	YES – AT CONTRACT STAGE
The school/setting will keep a record of all staff and children who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave	STAFF –SM Database PUPILS – SM Database
Assessing risks	
The school/setting 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 computer. Neither the school/setting nor Wandsworth Council can accept liability for the material accessed, or any consequences of internet access.	YES
The school/setting will audit ICT provision to establish if the e-Safety	YES

Policy is adequate and that its implementation is effective.	
Handling e-safety complaints	
Complaints of internet misuse will be dealt with by a senior member of staff.	YES – CATHERINE SHANLEY / MALCOLM MCKINLAY
Any complaint about staff misuse must be referred to the Principal/senior manager.	YES – CATHERINE SHANLEY / MALCOLM MCKINLAY
Introducing the e-Safety Policy to children	
e-safety rules will be posted in all networked rooms and discussed with children throughout the year	YES
Children will be informed that network and internet use will be monitored.	YES
Staff and the e-Safety Policy	
All staff will be given the e-Safety Policy and its importance explained.	YES – INDUCTION MTG W/ MCK & POLICY CHECKLIST (NW)
Enlisting parents' support	
Parents/carers attention will be drawn to the e-Safety Policy in newsletters, brochures and website.	YES

APPENDIX - ICT: 1

PARKGATE HOUSE SCHOOL ICT ACCEPTABLE USE POLICY

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

This policy is intended to ensure that:

- Pupils and staff will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the system and users at risk.

All staff will sign the ICT Code of Practice for Teachers and Adults when they join the school, and will be made aware of any amendments to the policy.

Pupils and their parents will be asked to sign the ICT Code of Practice for Pupils at the beginning of PP1 (year 1). Pupils (from PP1-Prep 6) entering the school at different times to those set out will be asked to sign the policy on joining the school.

PARKGATE HOUSE SCHOOL

STAFF ICT ACCEPTABLE USE POLICY & CODE OF PRACTICE

Staff access of internet and professional use

- All computer networks and systems belong to the school and are made available to staff principally for educational, professional and administrative purposes only.

- Staff are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.

- Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. If accessed accidentally users should report the incident immediately to the Principal or e-Safety coordinator.

- The school reserves the right to monitor internet activity and examine and delete files from the school's system.

- Staff have a responsibility to safeguard pupils in their use of the internet and reporting all e-safety concerns to the e-safety coordinator.

- Staff should only be accessing streamed information, i.e. radio, television, music, if it is of educational interest to a lesson or to its planning. Staff should only access streamed information and digital resources from the school's approved digital resource service: Espresso Education (an award winning, approved service that provides digital rich resources suitable for Key Stage 1 and Key Stage 2, for example cross-curricular multimedia resources and video clips). Staff and pupils are not permitted to view video through You Tube.

- Copyright and intellectual property rights in relation to materials used from the internet must be respected.

- E-mails and other written communications must be carefully written and polite in tone and nature.

- Anonymous messages and the forwarding of chain letters are not permitted.

- Staff should only access approved internet sites. The use of chat rooms and access to social networking sites, such as Facebook, Twitter etc., and blogs is not allowed and will be blocked.

- All email communications with parents must be sent directly from the school office email account. Unless given specific authorisation from the Principal, staff are not allowed to email parents, pupils or ex-pupils from either their school email account or personal email account. It is never acceptable to accept a "friendship request" from pupils at the school using a social networking site. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.

- Use of any portable media such as USB sticks or CD-ROMS is not allowed unless permission has been given by the network manager and a virus check has been carried out.

- Downloading executable files or unapproved system utilities will not be allowed and all files held on the school's system will be regularly checked.

- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

- Files should be saved, stored and deleted in line with the school policy.

- Staff are not permitted to allow unauthorised individuals access to the school's email, internet or school database.

Personal use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Use of the school's internet for financial gain (including the use of online auction sites), gambling, political purposes or advertising is not permitted.

- Teachers should not be accessing the internet for personal reasons whilst teaching children.

- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.

- School resources, such as software, are for the use of staff and pupils within the school premises and should not be taken home for personal use.

- Outside of school, staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute. Staff must recognise that it is not appropriate to discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct. Setting a high security level on social networking sites is advisable.

Use of mobile phones and personal cameras

- Mobile phones should not be used when teaching, unless in an emergency.

- Where it is recognised that members of staff may need to use their own telephone to contact each other, or relay information regarding expected arrival times from trips, any contact with parents should be undertaken though the school telephone system, i.e. parents should be discouraged from contacting members of staff on their mobile phones. All calls to staff regarding school business should be directed through the main school office.

- Staff are not permitted to use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission from the Principal, and are not permitted to store images at home without permission.

Use of the school's digital images

- It is not permitted for any photos or videos of pupils, staff or parents during any school activity (including educational visits and events) to be put on public display or published anywhere on the internet, including social networking websites.

- The above excludes the publication of photos on the school website or school newsletter for the purpose of school related marketing, by staff given direct authorisation to do this by the Principal; and also where a photo usage consent form has been signed by the parents concerned.

STAFF ICT ACCEPTABLE USE POLICY & CODE OF PRACTICE

USER AGREEMENT

I understand that it is my responsibility to ensure that I remain up-to-date and understand the school's most recent e-safety policies.

I agree to abide by all the terms and conditions set out in the above Staff Acceptable Use Policy and Code of Practice.

I would like to be able to use the school's ICT resources and systems; to have a school email account and if appropriate be connected to the school database.

Signature…………………………….……………….Date……………………………….

Full Name (printed)……………………………………..

Job Title………………………………………………….

PARKGATE HOUSE SCHOOL

PUPILS' ICT ACCEPTABLE USE POLICY & CODE OF PRACTICE

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I understand that I will be allowed to use the school internet if I use it responsibly. I understand that if I do not, I may not be allowed to use it.

I will:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable and will always report them to a teacher or parent. I know not to delete them straight away but show them to the person I reported it to, as evidence.
- not give my mobile number, home number or address to anyone who is not a real friend
- talk to my teacher before using anything on the internet
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.
- Not look for bad language, inappropriate images or violent games, and if I accidentally come across any I should report it to a teacher or parent. I know that my teacher can check the websites I have visited.
- not use personal e-mail, social networking sites, You Tube, or instant messaging in school.

- not use a personal mobile phone at school. If I bring a mobile phone to school I will take it to the school office on arrival.

- not download any software from the internet. I know that information the internet may not always be reliable and may need checking. I know that some websites may be sponsored by advertisers.

PARKGATE HOUSE SCHOOL

PUPILS' ICT ACCEPTABLE USE POLICY & CODE OF PRACTICE

PARENT FORM

Dear Parents,

Re: Pupils' ICT Acceptable Use Policy & Code of Practice

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Pupils from Pre-Prep 1 to Prep 6 will have supervised use of the internet, as directed by the teacher for the purposes of research and learning directly related to the curriculum. The school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and uses an approved content filtering system to safeguard pupils.

Whilst the school monitors ICT use in school it needs to be understood that children also have an important responsibility themselves as to how they use the internet and school equipment.

Please read through the pupils' ICT Acceptable Use Policy attached with your child and discuss with them the school rules relating to the use of ICT. Please complete and return the slip below to confirm that you have read, agreed and discussed the Pupils' ICT Acceptable Use Policy with your child.

ICT ACCEPTABLE USE POLICY – PUPIL AND PARENT AGREEMENT SLIP

I have read the Parkgate House Pupils' ICT Acceptable Use Policy with my child and we agree to abide by the terms and conditions set out in this policy.

To be completed by the parent:

Name of Pupil…………………………………….

Signature of Parent……………………….……………….Date……………………………….

To be completed by the pupil:

I have read the Pupils' ICT Acceptable Use Policy and agree to the rules set out in it.

Child's Name……………………………………………….

Other Relevant Polices

This policy should be read in conjunction with:
Discipline Policy
Suspension & Exclusion Policy
Health & Safety Policy
Safeguarding & Child Protection Policy
Anti-bullying Policy

Name of Policy Reviewer:	Catherine Shanley / Malcolm McKinlay / Nicola Willis
Date of Policy Review:	March 2013
Signature:	