PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

E-safety Policy
Whole school and EYFS

IMPORTANT: For the academic year 2021 – 2022, head/headteacher will be the Principal and therefore these titles are interchangeable.

The Head undertakes a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed: Mr Tim Cannell

Date reviewed: 6 September 2021

Date of next review: 3 September 2022

This policy should be read in conjunction with the School Safeguarding and Child Protection Policy

Aims:

- We will ensure that computers and other devices in school are subject to filtering and monitoring of internet usage.
- We will ensure that all staff and visiting staff accessing the computing system are aware and comply with our computing policies and agree to the Staff Acceptable Use of Computing Agreement.
- We will ensure that the use of mobile phones by staff and visitors adheres to our safeguarding procedures and staff guidelines.
- We will encourage the safe use of computers outside of formal lesson time – including any homework which is computing based.
- We will ensure that computer-based learning is age-appropriate and that children understand the dangers of internet usage through their PSHE and computing lessons.
- We will ensure that children are aware that the use of technologies to tease, bully or threaten is unacceptable.
- We will ensure that children and parents are aware of and sign up to the Child and Parental School Computing Agreement throughout their time in the school

Scope of the policy
This policy applies to all members of the Parsons Green Prep School who have access to the school computing systems.

The school will deal with inappropriate computing incidents within this policy and associated behaviour policy and will inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and responsibilities
Designated Safeguarding Lead

- has overall responsibility for e-safety in the school
- is responsible for establishing and reviewing the school e-safety policies/documents along with the Headteacher
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyberbullying
-

(N.B. It is important to emphasise that these are child protection issues, not technical issues. The technology provides additional means for child protection issues to develop).

Headteacher and senior leaders:

- The Head is responsible for the safety (including e-safety) of all members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Designated Safeguarding Lead (DSL).
- The DSL is responsible for ensuring that staff receive suitable training to enable them to follow and enforce his policy throughout the school.

The DSL:

- liaises with school technical staff
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides advice for staff
- provides updates for parents on important e-safety issues
- keeps up to date with e-safety technical information and advice in order to carry out their role effectively and inform and update others as relevant once a term
- reports regularly to the Headteacher
- ensures that all users of the school computing systems have signed and agreed to the Staff Acceptable Use of Computing Agreement.

This role is currently filled by the DSL in 2020-2021

External contractor (Alex Howard)

The technical staff are responsible for ensuring:

- liaison with school
- day-to-day responsibility for protecting against e-safety issues
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- that web filtering is updated on a regular basis
- that network and endpoint security systems are implemented and updated

Teaching and support staff

The teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the school's e-safety policy and practices in an annual e-safety inset day
- they have read, understood and signed the Staff Acceptable Use of Computing Agreement once a year or following any review (appendix 1)
- they report any suspected misuse or problem via email to the DSL

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

- all digital communications with children/parents/carers and staff should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- children and parents understand e-safety and follow the Child and Parental School Computing Agreement (appendix 2)
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Children

The children:

- are responsible for using the school computing systems in accordance with the Child and Parental School Computing Agreement (appendix 2)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyberbullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their attendance at the school.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, the website and further literature. Parents and carers are expected to act as a positive role model and will use social media responsibly in respect of all matters relating to the school. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines regarding:

- the appropriate use of digital and video images taken at school events
- their children's personal devices not being brought into school

Volunteers and peripatetic teachers:

Volunteers and peripatetic teachers who access school systems as part of the wider school provision will be expected to sign a Staff Acceptable Use of Computing Agreement before being provided with restricted access to school computing.

Education and training – staff/volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal e-safety training will be made available to staff either alone or as part of wider safeguarding training.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Staff Acceptable Use of Computing Agreement.
- This e-safety policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days.
- The DSL will provide advice/guidance/training to individuals as required.
- Participating in events/campaigns such as Safer Internet Day.
- Reference to the relevant websites/publications, e.g. www.swgfl.org.uk, www.saferinternet.org.uk and www.childnet.com/parents-and-carers.

Technical – infrastructure/equipment, filtering and monitoring

The school has a managed computing support service provided by an outside contractor. It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school e-Safety Policy and Staff Acceptable Use of Computing Agreement.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities, including:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Technical infrastructure must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The 'master/administrator' passwords for the school computing system, used by the external contractor and DSL, must also be available to the Headteacher upon request.
- The external contractor in liaison with the DSL is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is monitored for all children. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- An appropriate system is in place (an email to the DSL) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Regularly updated security measures are in place to protect the servers, network, endpoints and mobile devices from accidental or malicious attempts which might threaten the security of the school systems and data.
- Providing temporary access to 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Ensuring personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see Data Protection Policy).

Bring your own device (BYOD)

There are a number of e-safety considerations for BYOD that will be reviewed regularly. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- Parsons Green Prep has a set of clear expectations and responsibilities for all users.
- The school adheres to the principles of the Data Protection Act 1998.
- All users are provided with and accept the Staff Acceptable Use of Computing Agreement (appendix 1).
- All network systems are secure and access for users is differentiated.
- All users will use their username and password and keep this safe.
- The only devices which children may bring into school are reading tablets (ie kindles) and a mobile phone where the child walks to school. In both instances, permission must be sought from the form teacher (tablets) or headteacher (phones) first
- Any device brought in to school is done so at the owner's own risk.
- No chargers may be brought into school unless it has been PAT tested and has the correct sticker on it

Use of digital and video images

The school will inform and educate staff, children and visitors about the risks and will implement procedures to reduce the likelihood of the potential for abuse.

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, parents/carers should not share or make the images/video publicly available on social networking sites, nor should parents/carers make comments on any activities involving other children on social media.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should normally only be taken on school equipment.
- Where an image is taken using a staff device, the image must be downloaded to the school system and deleted from the device at the earliest opportunity
- Care will be taken when taking digital/video images that children are appropriately dressed (i.e. fully clothed) and are not participating in activities that might bring the individuals or the school into disrepute.
- Care will be taken not to publish any images with personal information on display, i.e. names or other background images.
- Photographs taken will not present any risk to the security of the school.
- Photographs published on the website or elsewhere that include children will be selected carefully and will comply with the consent form signed by parents at the start of each academic year (see appendix 4).
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

See the Data Protection Policy for more details.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service is be regarded as safe and secure and is monitored. Staff are aware that email communications may be monitored.
- Users must immediately report, to the DSL, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents/carers (email, chat, etc) must be professional in tone and content and in line with the school style guide. Personal email addresses, text messaging or social media must not be used for these communications.
- Children should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social media - protecting professional identity

All schools have a duty of care to provide a safe learning environment for children and staff. Staff members who harass, cyberbully, discriminate on the grounds of age, disability, gender, gender reassignment, religion or belief, race, sexuality, marital status or maternity or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- training to include acceptable use, social media risks, checking of settings, data protection, and reporting issues.
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk.

School staff should ensure that:

- other than on the school social media accounts and school website, no reference should be made on social media to students/children, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Monitoring

The DSL will keep a log of any incidents reported to him and E-safety will form part of any termly safeguarding review.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

At least once a term the DSL will (in concert with another adult for this purpose) test the school firewall to see that it is working correctly. The time of the test and the results of it should be noted by the DSL and the record signed by both parties taking part in the test.

Responding to incidents of misuse

Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the DSL immediately. If the incident concerns a member of staff, it should be reported to the Head.

In the event of suspicion, all steps in this procedure should be followed by the DSL:

- Have more than one senior member of staff/volunteer involved in this process, this is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by children and if necessary can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the reporting log (appendix 3) except in the case of images of child sexual abuse (see below).
- Once this has been completed and fully investigated the investigation group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
    - ‘extremism’, being vocal or active in opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Extremism also includes calls for the death of members of our armed forces, whether in this country or overseas.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

School actions and sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures – see the Behaviour Policy or Staff Handbook.

Reviewed and approved:	Job title: DSL
	6 September 2021
Next review due:	3 September 2022

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

APPENDICES

Appendix 1
STAFF ACCEPTABLE USE OF COMPUTING AGREEMENT

Staff use of the school's internet and email service

Whilst staff are encouraged to use email and the internet in support of their work, all use of these facilities should be appropriate to the work, standards and ethos of the school.

The use of the school's internet and email systems are not provided as a right to any of their users. They may be withdrawn from any user (adult or child) who does not conform to this Staff Acceptable Use of Computing Agreement. The school is responsible for authorising any user of its internet or email facilities, monitoring and policing their use.

Any member of staff who commits a serious offence in the use of the school's Internet service may be subject to the school's staff disciplinary procedures. Any user, adult or child, who breaks the law in respect of using the school's internet service will be reported to the police.

Personal use of the school's computing systems is not allowed. Printing of personal material, via download or mass storage device, is not permitted at any time.

Any member of staff found to be not adhering to these procedures will be issued with a verbal warning, in the first instance, after which the school's Disciplinary and Grievance Procedures will apply.

Staff or administrative users will protect the school from cyber threats or technical disruption by not downloading from the internet any programs or executable files other that by agreement with the school DSL.

INTERNET DOs & DON'Ts

DOS

- If you see any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up widow or in any other way, report it immediately to the DSL.
- Staff or approved adult school users should at all times abide by the **copyright laws** in respect of documents and materials downloaded from the internet.
- Staff using a school laptop or other device off the school site, at home or elsewhere, will still have to abide by the school Internet Acceptable Use of Computing Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the **Computer Misuse Act 1990.**
- Staff will at all times work to maximise the safety of children within their care in their use of the internet.
- Staff will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any internet material or work with the internet in any way that infringes or offends these.

DON'TS:

- Don't log on to the network with another user's account.
- Don't alter the settings of computers or make other changes which make them unusable by others.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

- Software may only be installed by the school's IT department.
- Don't download classroom resources or materials if you are unsure about their suitability.
- Never pass on, or make obvious, or leave in an insecure place any passwords associated with using the internet, email or computer system.
- Don't procure goods or services directly over the internet without the prior, specific agreement of the Headteacher
- Don't provide personal details or contact details of your own, or any other person, to internet sites including weblogs, forums or chat rooms. Exceptions should be checked with the Headteacher
- Don't upload an image to a website without complying with guidance on images loaded to the internet.

The school will maintain a record of all staff and children who are provided with internet access via the school's internet service. This record will be kept up to date and be designed to handle common eventualities such as a member of staff leaving or a child's access being withdrawn, etc.

The Staff Acceptable Use of Computing Agreement for all school staff and approved adult users of the school will be posted, and/or made available, in all rooms and offices where staff computers are used.

Staff use of the school's email service

DOs

- Do remember that sending an email from your Parsons Green Prep account is similar to sending a letter on PGP headed paper. It is your responsibility to maintain professionalism at all times and to ensure that you do not in any way bring discredit or embarrassment to the school.
- Do check your email regularly - ignoring messages is discourteous and confusing to a sender.
- Do treat the content of any email or an attachment that you prepare in the same way as any other paper-based letter or document from a legal point of view. The laws of the land apply equally to electronic messages and documents as they do to paper documents, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. Remember it is easy for your email to be passed on electronically to others should any recipient decide to do so.
- Do keep a copy of all incoming pupil-related emails and forward them to admin@parsonsgreeprep.co.uk - delete all others, e.g. personal emails, spam etc.
- Do keep email messages as brief as possible.
- Do make sure that the 'subject' field of any email that you send is meaningful and representative of the message it contains.
- Do make sure that your email address is included on any contact information put onto paper-based letters or documents.
- Do ensure that any email received by a member of staff which is regarded as illegal or offensive is reported to the Headteacher immediately. Similarly, any email received by a child which is regarded as illegal or offensive should be reported to the Headteacher immediately.
- Do refer to the school style guide when composing an email communication.
-

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

DON'Ts

- The school's email system should not be used by any user (adult or child) for the sending of personal mail unconnected with school work or activity.
- To safeguard against computer viruses do not open external emails or email attachments that look in any way suspicious - report them to the DSL.
- Never open an attached program file with a file extension of 'exe', 'com' or 'bat' sent to you with an email unless you are absolutely certain that it has come from a trusted source. All such files must be thoroughly virus-checked before they are opened.
- Do not make changes to someone else's email and then pass it on without making it clear where you have made the changes. This is a form of misrepresentation.
- Do not copy images or any other material for use in your email or an attachment that infringes copyright laws.
- Do not attach large documents (e.g. a document greater than 15 pages long) to an email. Take great care with multiple attachments that they do not present an unacceptable accumulated email size to the email system.
- Do not, under any circumstances, give your email password to anyone else.
- Do not print out all your email messages as a matter of course. Only print those for which it is an absolute necessity to do so.
- Do not broadcast an email to any group of recipients unless it is absolutely necessary. Also, never send or forward chain email.
- Unless you are authorised to do so, do not send an email to any supplier that could be interpreted as creating a contract in any way. In general, do not use emails for contractual purposes. N.B. Within the law, a user could send an email contain wording which may form a legally binding contract with a supplier.
- Do not create email congestion by sending trivial messages or by copying emails to those who do not need to see them.
- Do not attempt to read another person's email.
- Take care not to reply to a whole group when responding to an email sent to a group of recipients unless absolutely necessary.

Passwords

- Staff passwords should be changed immediately on suspicion of a breach.
- Passwords must have 6 characters or more, one capital letter and one number.
- Changes to your email and computer passwords should be made by completing a password change request form via the DSL.

Other forms of computing

Mobile telephones

- Personal mobile telephones may only be used in the staff room or in the school office or in a classroom where no children are present.
- Personal mobile telephones should be switched off or in 'silent' mode and stored securely when outside of the designated areas.
- The use of personal mobile phones is not allowed in any place whilst contact with children is taking place.
- Mobile telephones must be kept in a lockable drawer or in the staff room.

Television/DVD/Video

- Any content intended to be shown to children must be previewed to assess its suitability.

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

- In the case of certified films, parental consent must be sought before using films with a PG (Parental Guidance) certification.

Wifi-enabled devices.

- The school computing systems refers also to the Parsons Green Prep wifi connection.
- Any visitor or member of staff connected to the schools wifi connection must adhere to the Acceptable Use of Computing Policy.
- Only the school's guest wifi connection may be use mobile phones or personal devices.

Mass Storage Devices

- Any member of staff using a mass storage device must do so securely and use password encryption for access to the device. This password must be made available to the DSL.
- Mass storage devices containing any confidential information relating to the school, its staff or students must be password protected.
- Mass storage devices containing files for anything other than professional use must not be used on the school's computing system.

STAFF ACCEPTABLE USE OF COMPUTING AGREEMENT
I have read and agree to adhere to the school's Staff Acceptable Use of Computing Agreement and guidelines.

Signed: **Date:**

Print Name:

Position:

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

Appendix 2
Child and Parental School Computing Agreement

- Ask a teacher or suitable adult if you want to use the computers.
- Only use activities that a teacher or suitable adult has told or allowed you to use.
- Take care of the computer and other equipment.
- Ask for help from a teacher or suitable adult if you are not sure what to do or if you think you have done something wrong.
- Tell a teacher or suitable adult if you see something that upsets you on the screen.
- Make sure you follow all our school computer rules.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……Date……..

As a responsible parent, I support the school policies on digital technology and the internet. I monitor my child's use of the internet and social media outside of school. I will also act as a positive role model and will use social media responsibly in respect of all matters relating to the school.

Parents and carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, parents/carers should not share or make the images/video publicly available on social networking sites, nor should parents/carers make comments on any activities involving other children on social media.

Signed (parent): ……Date……..…..

PARSONS GREEN PREP SCHOOL
1 Fulham Park Road, London SW6 4LJ
T: 020 7371 9009
E: office@parsonsgreenprep.co.uk

Appendix 3
Reporting log

Reporting Log
Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		