Primrose Hill Primary School

Online Safety Policy

Based on Camden's Model Online Safety Policy for Schools

November 2021

This policy is in the process of being ratified by the Curriculum and Pupil Welfare Committee, on behalf of the Primrose Hill Primary School Full Governing Body.

Contents

Key contacts

Name of school:
Primrose Hill Primary School

Headteacher:
Name: Phil Allman
Contact details:
020 7722 8500

Online safety co-ordinator:
Name: Phil Allman
Contact details:
020 7722 8500

Nominated LGfL contact:
Name: Alex Marinos
Contact details:
suppoort@camdensitss.org

IT systems/Data manager:
Name: Alex Marinos
Contact details:
support@camdensitss.org.uk

Designated safeguarding lead:
Name: Liz Ghamar
Contact details:
020 7722 8500

Nominated governor:
Name: Isabel Murphy
Contact details:
020 7722 8500

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO):
Name: Sophie Kershaw/John Lawrence-Jones
Contact details: 020 7974 4556

Child and Family Contact/MASH team:
Manager: Jade Green
Tel: 020 7974 1553/3317
Fax: 020 7974 3310

Camden online safety officer:
Name: Jenni Spencer
Tel: 020 7974 2866

Prevent Education Officer
Name: Jane Murphy
Tel: 020 7974 1008

1 Information on internet technology

1.1 Introduction

Primrose Hill School believes that the educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. We believe we should teach children how to keep themselves safe whilst on-line.

We strive to continually develop an effective online safety strategy so that these aims can be achieved and that it will support staff in recognising the risks, and in taking action, to help children use the internet safely and responsibly.

Our online policy will be communicated to staff, pupils and parents and the policy document should be posted on the school's website.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as online bullying. More details on this can be found in section 4.5 of this policy.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- online bullying (see section 4.5 for further details)
- use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

2 School online safety strategies

2.1 Whole school approach

Computing is now a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Primrose Hill School considers the following in order to ensure a holistic approach to online safety:

- Staff are made aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and are made aware of the use of technology in peer on peer abuse.
- When developing new policies, Primrose Hill School ensures online safety and the impact of technology is considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.
- Primrose Hill School ensures that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff will receive suitable training around online safety and similar messages are taught to pupils.
- Staff are made aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with pupils, and we ensure there are clear policies available to staff on expectations for online behaviour.
- There is a clear link between the online safety policy and the behaviour policy that sets out expected standards for pupil's online behaviour and expected sanctions for breaches.
- Primrose Hill School's online safety policies are reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

We refer to:

DfE non-statutory guidance on teaching online safety:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE:
https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

2.2 Purpose and description

Primrose Hill School has an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

In Primrose Hill School we strive to ensure the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (the London Grid for Learning platform).
- A culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of on-line behaviour.
- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

2.3 Roles and responsibilities

Primrose Hill School recognises that a successful online safety strategy needs to be inclusive of the whole school community, including teaching assistants, HLTAs, governors and others, as well as forging links with parents and carers. The strategy has the backing of school governors, is be overseen by the head teacher and fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Head teacher's role

Head teachers have ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

2.3.2 Governors' role

The Governing body has a statutory responsibility for pupil safety and should is therefore aware of online safety issues, providing support to the head teacher in the continual development of the school's online safety strategy.

Governors ensure that there are policies and procedures in place to keep pupils safe online and these are reviewed regularly.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

2.3.3 Online safety co-ordinator's role

Primrose Hill School has a designated online safety co-ordinator who is responsible for co-ordinating online safety policies on behalf of the school. Our online safety coordinator is the head teacher.

The online safety co-ordinator has the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's online safety policy
- ensure that staff and pupils are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- ensure that all staff and pupils have read and signed the acceptable use policy (AUP)
- report annually to the board of governors on the implementation of the school's online safety strategy
- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues to Camden's online safety officer.

In addition, it is an Ofsted recommendation that the online safety co-ordinator receives recognised training CEOP or E-PICT in order to carry out their role more effectively. In Camden, this is available from the CLC.

2.3.4 Network manager's role

Primrose Hill School uses the Camden IT support service to manage our network. This includes:

- the maintenance and monitoring of the school internet system including anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the online safety co-ordinator
- supporting any subsequent investigation into breaches and preserving any evidence.

2.3.5 Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's online safety and acceptable use policy and procedures
- communicating the school's online safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the online safety co-ordinator
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator
- teaching the online safety and digital literacy elements of the new curriculum.

2.3.6 Designated safeguarding leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the school who will decide whether or not a referral should be made to Children's Safeguarding and Social Work or the Police.

2.4 Pupils with special educational needs and disabilities (SEND)

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. Primrose Hill School has a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

SEND co-ordinators are responsible for providing extra support for these pupils and they:

- link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- ensure that the school's online safety policy is adapted to suit the needs of pupils with SEND
- liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.

2.5 Working with parents and carers

Primrose Hill School believes it is essential to involve parents and carers in the development and implementation of online safety strategies and policies; most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

Primrose Hill School offers online safety training opportunities to parents in order to provide them with information to help them keep their child safe online. The CSCP online safety leaflet for parents is also available on the school website: https://cscp.org.uk/wp-content/uploads/2019/06/Online_Safety_Leaflet_for_Parents.pdf

The head teacher, board of governors and the online safety coordinator (at present this is the head teacher) work together to consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home. This includes information on the school website, in the weekly newsletter and workshops for parent.

Parents are provided with information on computing and the school's online safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Parents also know that they can contact the school's online safety co-ordinator if they have any concerns about their child's use of technology.

3 Online safety policies

3.1 Accessing and monitoring the system

- Access to the school internet system is via individual log-ins and passwords for staff and pupils wherever possible
- Staff are required to change their password regularly by LGFL and Camden IT
- Network and technical staff responsible for monitoring systems are supervised by a senior member of their management team.
- The online safety co-ordinator, the computing lead and teaching staff carefully consider the location of internet enabled devices which children use in the school in order to allow an appropriate level of supervision of pupils.

3.2 Confidentiality and data protection

- Primrose Hill School ensures that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.
- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School. Any breaches of data security should be reported to the online safety co-ordinator immediately.
- Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.

3.3 Acceptable use policies

- All internet users within the school are expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.
- For pupils, we have age appropriate acceptable use agreements which are signed by every pupil. Parents also sign acceptable use agreements and give consent for their child to have access to the internet in school (see appendices 1a, 1b, 1c and 2).
- Staff, Governors and Volunteers must also sign an acceptable use policy on appointment and this will be integrated into their general terms of employment / service (see appendices 3 and 4).
- Visitors and Contractors are also expected to sign an acceptable use policy where it is deemed relevant for them to do so (see appendix 4)

The School Business Manager will keep a copy of all signed acceptable use agreements.

3.4 Teaching online safety

3.4.1 Responsibility

One of the key features of Primrose Hill School's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use.

- Overall responsibility for the design and co-ordination of online safety education lies with the head teacher, but all staff should play a role in delivering online safety messages.
- The head teacher is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used is an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Primrose Hill School teaches about online bullying as part of statutory Relationships Education and health education.
- PSHE lessons provide an opportunity for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.
- Teachers are aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills for example pupils with SEND.
- Teachers ensure that the school's policy on the prohibited use of pupils' own mobile phones and other mobile devices in school is adhered to.

3.4.2 Content

At Primrose Hill School pupils are taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- can begin to evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- become responsible, competent, confident and creative users of information and communication technology.

Pupils are taught all elements of online safety included in Statutory Relationships Education, including:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help
- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met

- how information and data is shared and used online.

Statutory Health Education includes:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- why social media, some computer games and online gaming, for example, are age restricted
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- where and how to report concerns and get support with issues online.

3.5 Staff training and conduct

3.5.1 Training

Primrose Hill School staff and governors receive training with regard to IT systems and online safety as part of their induction.

Staff should also attend specific training on online safety available from the CSCP and other recognised providers (e.g. CLC, ECP)so that they are aware of the risks, and actions to take, to keep pupils safe online. Senior management ensure that staff attend or receive regular updates and training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

3.5.2 IT and safe teaching practice

Primrose Hill School staff are aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils. Staff refer to the Camden Model Schools Social Media Policy for school staff for further guidance.
https://cscp.org.uk/professionals/schools-and-nurseries-safeguarding-policies/

The following points must be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips
- Staff must always use school equipment and only store images on the school computer system, with all other copies of the images on personal mobile devices erased
- Staff must take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these
- Staff must ensure that any materials published on their own social networking sites are neither inappropriate nor illegal
- Staff must be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality
- Staff must not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute
- Staff must not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context
- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils
- Parents should never be given personal email address. They can contact teachers by using the school admin email address
- Staff should ensure that personal data relating to pupils is stored securely if taken off the school premises
- Where staff are using mobile equipment such as laptops or tablets provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5.3 Exit strategy

When staff leave, the School Business Manager will ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

3.6 Safe use of technology

3.6.1 Internet and search engines

- When using the internet, children receive the appropriate level of supervision for their age and understanding. Teachers are aware that often, the most computer-literate children are the ones who are most at risk

- Children are supervised at all times when using the internet
- Pupils are not allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety co-ordinator, who will liaise with the IT service provider for temporary access, if possible. Teachers should notify the online safety co-ordinator once access is no longer needed to ensure the site is blocked.

3.6.2 Evaluating and using internet content

Teachers teach pupils good research skills that help them to maximise the resources available on the internet so that they can increasingly use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

Primrose Hill School's email system is hosted by an email system that allows content to be filtered and allows pupils to send emails to others within the school or to approved email addresses externally.

Social networking sites such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has access to the site. The use of these are restricted/blocked in school, but pupils are likely to use these sites at home.

Online communities and forums are sites that enable users to discuss issues and share ideas on-line. Primrose Hill School may feel, if appropriate, that these have an educational value, but **each** visit to such sites must be approved by the head teacher.

Chat rooms are internet sites where users can join in "conversations" on-line; **instant messaging** allows instant communications between two people on-line. In most cases, pupils will use these at home but Primrose Hill School does not allow the use of these.

Gaming-based sites allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites are not accessible via school internet systems

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the school internet system is forbidden and is usually blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- If there is a clear educational use for emails or social networking sites and forums for on-line publishing, only approved sites such as those provided by the IT service provider may be used. Any use of these sites will be strictly supervised by the responsible teacher.

- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- Apart from the head teacher, individual email addresses for staff or pupils are never published on the school website.

- Pupils are be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

- Pupils are taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.

- All electronic communications must be polite; if a pupil receives an offensive or distressing email or comment, they have been instructed not to reply and to notify the responsible teacher immediately.

- Pupils are warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This includes any correspondence or contact taking place outside the school and/or using non-school systems or equipment.

- Users are aware that as use of the school internet system is for the purposes of education or school business only, its use may be monitored.

- In order to teach pupils to stay safe online outside of school, they are advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    - to only use moderated chat rooms that require registration and are specifically for their age group
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else

- not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room
- to behave responsibly whilst on-line and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.6.4 Video calling and remote learning

Video calling or live streaming enables users to communicate face-to-face via the internet using web cameras.

Primrose Hill School has a remote learning policy which was created in line with the DfE and London Grid for Learning guidance. The following should be taken into account:
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- only using school registered accounts rather than personal accounts
- the security of the video link
- checking settings regularly to ensure teachers have full control of the meeting ie; who can start, join or chat in the stream
- paying attention to background settings to prevent breach of privacy
- training for teachers to use the new technology
- a system for teachers to log any remote learning contacts and issues.

Further guidance on remote learning can be found on the London Grid For Learning website: https://edtech-demonstrator.lgfl.net/

Live sessions are not recorded due to data protection laws and reluctance of many parents to give consent.

3.6.5 School website

- All teachers are authorised to upload material on to the school website. They understand that content must be accurate, suitable etc. They know to check with the online safety co-ordinator if they are unsure about any particular material
- To ensure the privacy and security of staff and pupils, the contact details on the website are the school address, email and telephone number. No contact details for staff or pupils are contained on the website
- Children's full names should never be published on the website
- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.6.6 Photographic and video images

- Written permission is obtained from parent/carers when their child joins the school as to whether or not they consent to photos or videos of their child being taken and used on the school website or newsletter. Consent can later be withdrawn at any time.
- Children's names are never published where their photograph or video is being used.
- Staff ensure that children are suitably dressed to reduce the risk of inappropriate use of images.
- Images are securely stored only on the school's computer system and all other copies deleted.
- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.
- Staff must not use personal devices to take photographs of pupils.
- Primrose Hill School informs parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

3.6.7 Pupils own mobile devices

Many pupils are likely to have mobile phones or other devices that allow them to access internet services. While Primrose Hill School allows children to bring a mobile phone to school, it must be left securely locked away by their class teacher or the main office during school hours. If older children are permitted to walk to and from school alone, many parents prefer their children to have mobile phones with them in order to ensure they have arrived at school safely and let them know when they are on their way home. The use of personal mobile phones or other devices are be forbidden in classrooms without the express permission of the head teacher.

We are aware that it is considerably more difficult to monitor wireless devices. No such devices should be brought in to school at any time. Any use of the school's handheld devices such as tablets which are given to pupils by schools for education purposes will be closely monitored by the responsible adult.

All access to the internet is via the school's devices. Should an occasion arise when pupils can access the school internet system via their own devices, it must be made clear to pupils that the same acceptable use agreements apply and that sanctions may be applied where there is a breach of school policy.

Where a pupil's device is used for bullying or sexual harassment, the school policy will be followed, which allows the device to be confiscated so that evidence can be gathered. In such a case we would refer to the government guidance available at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

See the Staff Acceptable Use Agreement/Policy regarding to staff use of their own mobile devices whilst school.

RELATED POLICIES:
Acceptable Use Agreement
Staff Code of Conduct Policy
Behaviour Policy
Anti-bullying Policy
Social Media Policy

4 Responding to incidents

4.1 Policy statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety co-ordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety co-ordinator on the online safety incident report form (appendix 5).
- A copy of the incident record should be emailed to Camden's designated online safety officer at jenni.spencer@camden.gov.uk.
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action under staff conduct policies for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors.
- The online safety co-ordinator should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.
- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated safeguarding lead, who will make a decision as to whether or not to refer the matter to the police and/or Children's Safeguarding and Social Work in conjunction with the online safety co-ordinator.

Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.
- The incident should be reported to the online safety co-ordinator and details of the website address and URL provided.
- The online safety co-ordinator should liaise with Camden SITSS to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

4.3 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).
- The incident should be reported to the online safety co-ordinator and details of the website address and URL recorded.
- The Online safety co-ordinator should liaise with CamdenSITSS to ensure that access to the site is blocked.
- The pupil's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher immediately. If the misconduct involves the head teacher or a governor, the matter should be reported to the chair of governors.
- The head teacher will notify Camden SITSS so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.
- The head teacher will arrange with CAMDEN SITSS to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established, the head teacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.
- If the materials viewed are illegal in nature the head teacher or governor should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.

4.5 Online bullying

4.5.1 Definition and description

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, sexting/"happy slapping").

Online bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school. All incidents should be dealt with under the schools' behaviour policies and the peer on peer abuse guidance. https://cscp.org.uk/professionals/schools-and-nurseries-safeguarding-policies/

- Primrose Hill School Anti-bullying Policy, Behaviour Policy and Acceptable Use Policy cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach.
- Any incidents of online bullying should be reported to the online safety co-ordinator who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school's Anti-bullying Policy. Incidents should be monitored and the information used to inform the development of the Anti-bullying Policy.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.
- As part of online safety awareness and education, pupils are told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.
- Pupils are taught:
    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to send or post inappropriate images of themselves
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts and the threat is serious, the police may become involved and can ask the mobile phone company to trace the calls. The pupil should also consider changing their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, we will suggest that parent / carers contact the service provider so that the sender can be traced. The pupil should also consider changing email address.
- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves messages on social networking sites or blogs, we will suggest that the parent/care contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked and police can become involved.
- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Online bullying of school staff

- The Head teachers is aware that school staff may become victims of online bullying by pupils and/or their parents. Because of the duty of care owed to staff, the head teachers ensures that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents.
- The issue of online bullying of school staff is incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.
- Incidents of online bullying involving school staff are recorded and monitored by the online safety co-ordinator in the same manner as incidents involving pupils.
- Staff should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.
- Personal contact details for staff must never be posted on the school website or in any other school publication.
- Staff must follow the advice above on online bullying of pupils and not reply to messages but report the incident to the head teacher immediately.
- Where the bullying is being carried out by parents the head teacher will contact the parent to discuss the issue. Our Home / School Agreement can be referred to to ensure responsible use.

4.6 Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying.

Primrose Hill School is aware that the following online behaviours of a sexual nature could constitute harmful behaviour:

- sharing explicit and unwanted content and images
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats.

Primrose Hill School is aware of the duty under statutory guidance Keeping children safe in education and Sexual violence and sexual harassment between children in schools and colleges.

This requires us to have policies in place to deal with incidents of on-line sexual harassment. The school refers to the Peer on peer abuse and sexual violence and harassment guidance for schools and colleges for further details. https://cscp.org.uk/professionals/schools-and-nurseries-safeguarding-policies/

It is recommended that the school makes pupils aware that producing and distributing sexual images to peers via the internet or mobile devices may be illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

It is important to be mindful that any of these behaviours may possibly be linked to the sexual exploitation of a pupil or is being carried out as a gang-related activity. Staff should refer to the CSCP child sexual exploitation guidance for further details. http://www.cscb-new.co.uk/wp content/uploads/2015/09/Multi_Agency_Guidance_On_Child_Sexual_Exploit tion_2015.pdf

4.7 Risk from inappropriate contacts with adults

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

Staff should be mindful that some pupils can be sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts must be reported to the online safety co-ordinator and the designated safeguarding lead.
- The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Children's Safeguarding and Social Work and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
- The designated safeguarding lead can seek advice on possible courses of action from Camden's online safety officer in Children's Safeguarding and Social Work.

- Teachers will advise the pupil on how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated safeguarding lead and the online safety co-ordinator will always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school IT equipment or networks, the online safety co-ordinator will make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.8 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff have been trained on the school's duty under the Prevent programme and are able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff have been warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.
- The school ensures as far as possible, through CamdenSITSS monitoring, that adequate filtering is in place and will review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents are dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures will be used as appropriate.
- The online safety co-ordinator and the designated safeguarding lead record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are, and this is placing the child or young person at risk, Primrose Hill School will refer the young person to the MASH. Guidance can also be sought from the Prevent Education Manager.

Further information is available in the CSCP guidance "Safeguarding children and young people from radicalisation and extremism" available at: https://cscb-new.co.uk/?page_id=8128

4.9 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- Pstoral support is always available to pupils to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Members of the Inclusion Leadership Team, which includes the Pastoral Lead, have received training needed support issues such as self-harming, suicide, substance misuse and anorexia should they arise and would make appropriate referrals as necessary.

5 Sanctions for misuse of school IT

Primrose Hill School will apply sanctions for breach of acceptable use policies. Sanctions applied reflect the seriousness of the breach and take into account all other relevant factors. The school uses the framework recommended by LGfL.

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

These low-level breaches could include referral to the Phase Leader, the Pastoral Lead or a referral to the Online Safety Coordinator.

Sanctions could include:

- Time Out
- Reflection
- Telephone call home.

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to the Phase Leader
- Referral to the Pastoral Lead
- Reflection
- referral to online safety co-ordinator
- loss of internet access for a period of time
- contacting parents.

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- online bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to Phase Leader
- Referral to Pastoral Lead
- Reflection
- referral to online safety co-ordinator
- referral to head teacher (if different)
- loss of access to the internet for a period of time
- contact with parents
- any sanctions agreed under other school policies.

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme online bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's online safety officer.

5.2 Sanctions for staff

Sanctions should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the staff behaviour policy or code of conduct.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher as a low level incident in line with the school's staff conduct policy.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the head teacher who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO under the CSCP guidance on dealing with allegations against staff and volunteers.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Possible sanctions include:

- referral to the head teacher
- removal of equipment
- referral to Camden's online safety officer
- referral to Camden's LADO or the police
- suspension pending investigation
- disciplinary action in line with school policies.

RELATED POLICIES:

School's Disciplinary Policy
Staff Code of Conduct Policy
Guidance on Dealing with Allegations Against Staff

Appendix 1a:

ONLINE SAFETY - ACCEPTABLE USE POLICY & AGREEMENT

For Nursery, Reception and Years 1 to 3 Pupils

Please read carefully, discuss with your child, then *your child* must tick the boxes and sign / mark the attached agreement. Please return it to the school office.

Child's full name _____ Class: _____

To stay **SAFE online and on my devices:**	✓
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:_____ at school

_____ at home

Child to sign / write / mark their name: _____ Date: _____

Appendix 1b

ONLINE SAFETY - ACCEPTABLE USE POLICY & AGREEMENT

Years 4, 5 and 6 Pupils

Please read carefully, discuss with your child, then *your child* must tick the boxes and sign the attached agreement. Please return it to the school office.

Pupil Agreement

1. ***I learn online*** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

2. ***I learn even when I can't go to school because of coronavirus*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.

3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.

5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.

11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. ***I say 'no' online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

16. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.

17. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

18. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

19. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

20. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

21. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

22. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

23. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

CHILD'S FULL NAME: _____Class: _____

I have read and understood this agreement and I will use the computers, internet and other new technologies in a responsible way at all times.

If I have any questions, I will speak to a trusted adult at school.

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed by pupil: _____ Date: _____

Appendix 1c

ONLINE SAFETY - ACCEPTABLE USE POLICY & AGREEMENT – Symbols

Please read carefully, discuss with your child, then *your child* must tick the boxes and sign the attached agreement. Please return the signed agreement to the school office.




What I Must do to Keep Safe Online and With Devices

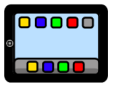


Online means anything connected to the internet. Most devices and


apps are connected to the internet.



Devices are technology like: computers, laptops, games consoles,

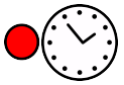


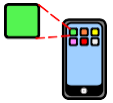

tablets and smart phones.




I will only use the devices I am allowed to use.



I will ask a trusted adult before I use new websites, games or apps.

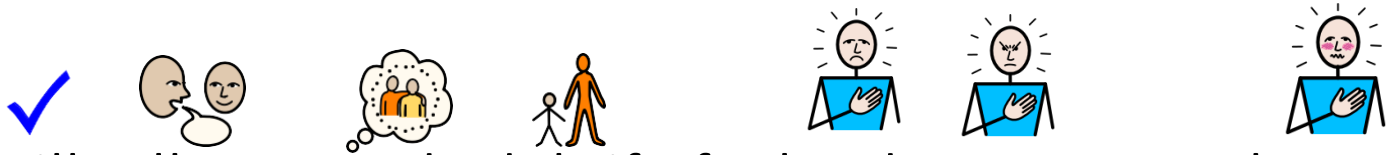




I will ask for help if I'm stuck or not sure.

I will be kind and polite to everyone online.

I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.

I will tell a trusted adult if I feel bad or unsafe when I am using a device.

I know people online sometimes tell lies.

They might lie about who they are or where they live.

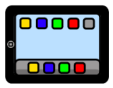



I never have to keep secrets from my trusted adults.









I will not change clothes or undress in front of a webcam.

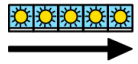





I will always ask a trusted adult before telling anyone my private

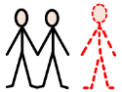
information or location.





I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.


This could make me feel sad or embarrassed.



My trusted adults are _____ at school



My trusted adults are _____ at home


My name is _____ Date:_____

Appendix 2

ONLINE SAFETY - ACCEPTABLE USE POLICY & AGREEMENT

Parents / Carers

All children and adults involved in the life of Primrose Hill are required to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Enclosed with this parent/carer agreement, you will also find an age-appropriate agreement for your child to sign. Please read and discuss their agreement with them, and return both parent/carer and pupil signed agreements to the school office.

We tell your children that **they should not behave any differently when they are out of school or using their own device or home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?
You can read Primrose Hill's full **Online Safety Policy** on our website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this Acceptable Use Policy or our approach to online safety, please speak to our Online Safety Coordinator Phil Allman (Head teacher).

What am I agreeing to?

1. I understand that Primrose Hill uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

7. I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screen time and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...

8. **I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.**

9. **If my child has online tuition for catch-up after lockdown or in general, I will refer to** the Online Tutors – Keeping children Safe poster and **undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them**.

10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.

11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/

12. **I understand and support the commitments made by my child in the Acceptable Use Policy and Agreement (AUP) which they have signed.**

The Child Exploitation and Online Protection (CEOP) website is the government's official resource to assist both teachers and parents in explaining to children the benefits and risks associated with digital media.

This is a good place to start for parents who are unsure about how to tackle this important subject, and has a useful section for parents and carers: http://www.thinkuknow.co.uk

I have read, understood and agree to this policy. ***Please complete below and return copy to school ASAP***

Parent / Carer Signature: _____

Name of Parent / Carer: _____

Parent / Carer of (Pupil's Name & Class): _____

Date: _____

Appendix 3

ONLINE SAFETY ACCEPTABLE USE AGREEMENT

Staff and Governors

This agreement covers use of digital technologies both in school and when accessing remotely, and includes: email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone. Supply teachers will be provided with their own logons.
- I will not allow unauthorised individuals to access email / Internet / network/ LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business (currently LGfL Staffmail).
- I will only use the approved school email or other school approved communication systems with colleagues, pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the online safety co-ordinator (see the school's Online Safety Policy).
- I will not intentionally download any software or resources from the Internet that can compromise the network or are not adequately licensed.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- If using a USB flash drive outside school, it must be encrypted, and I will frequently use anti-virus software to scan it for viruses.
- Mobile devices (mobile phones, tablets and other mobile devices) brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or put on silent at all times – unless explicit permission has been granted by the head teacher for use in specific situations.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission from the Head teacher.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and are not accessed at school. I will ensure permissions are set to limit access and that any information within these sites is appropriate.
- I agree and accept that any computer or laptop loaned to me by the school, is provided to support my professional responsibilities and is not for personal use.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- Teaching staff: I will embed the school's online safety curriculum into my teaching.
- I will only use Local Authority systems in accordance with any corporate policies.
- **I understand that failure to comply with this agreement could lead to disciplinary action**.

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

I understand that all online safety policies and procedures apply to my professional conduct both in school and remotely. I have read this agreement in conjunction with Primrose Hill's Remote Learning Offer, available on the school website:
https://www.primrosehill.camden.sch.uk/wp-content/uploads/2021/02/Remote-Learning-Offer-2021.docx.pdf .

I agree to abide by all the points above.

I wish to have an email account, be connected to the network & Internet and be able to use the school's ICT resources and systems.

Signature …… Date ……

Full Name …….. (printed)

Job title ……

Please complete and sign above and return to Julia Chalfen, the School Business Manager

Authorised Signature (Head Teacher)

I approve this user …….. (Name of member of Staff / Governor)

to be set-up to access and use the school ICT resources.

Signature …… Date ……

Full Name …… (printed)

One copy is retained by member of staff | Second copy for school file

Appendix 4:

ONLINE SAFETY ACCEPTABLE USE AGREEMENT

Volunteers, Contractors and Visitors

Volunteers, contractors and visitors (where relevant) are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask.

Further details of our approach to online safety can be found in the overall school Online Safety Policy, available on the school website.

If you have any questions during or after your visit, please ask the person accompanying you (if appropriate) or the School Business Manager, Julia Chalfen.

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's security, monitoring and filtering systems and/or viewed by an appropriate member of staff.

2. I will never attempt to arrange **any** meeting without the full prior knowledge and approval of the school and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

3. **I will leave my phone in my pocket** and turned off. **Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils.** If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher or school business manager and it will be done in the presence of a member staff.

4. If I am given access to school-owned devices, networks, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
    - I will not attempt to make contact with any pupils or to gain any contact details under any circumstances
    - I will protect my username/password and notify the school of any concerns
    - I will abide by the terms of the school Data Protection Policy and GDPR protections https://www.primrosehill.camden.sch.uk/wp-content/uploads/2021/10/Data-Protection-Policy-July-2021.pdf

5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.

6. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.

7. I will not do or say anything to undermine the positive online safety messages that the school disseminates to pupils.

8. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead Elizabeth (Liz) Ghamar (if by a child) or to the Headteacher Phil Allman (if by an adult).

9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the Volunteer / Contractor / Visitor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date: _____

Appendix 5:

Online Safety Incident Report Form
This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

School/organisation's details:

Name of school/organisation:

Address:

Name of online safety co-ordinator:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (online bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
□ terrorist material
□ online grooming
□ online radicalisation
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ online bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to head teacher/senior manager
□ advice sought from LADO
□ referral made to LADO
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to head teacher/senior manager
□ advice sought from Children's Safeguarding and Social Work
□ referral made to Children's Safeguarding and Social Work
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ online safety policy to be reviewed/amended

Outcome of incident/investigation