Online Safety and Acceptable User (including Cyber Security) Policy

Date	Review Date	Headmistress	Proprietor
October 2023	October 2026	Miss Danica Belzer	Mr Brian Berkery

Online Safety Coordinator
Hannah Roberts Deputy Headmistress (also DSL)

Online Safety (also referred to as e-safety) encompasses not only the internet but also wireless communications including mobile phones, cameras, webcams, iPads, eBooks and PC tablets. Online safety also includes the consideration of media applications and a user's access to content and contact with others such as chat rooms, blogs, social networking sites, instant messaging, gaming and video broadcasting.

Safeguarding is everybody's responsibility and therefore an agreed, shared approach must be promoted by all staff, parents and children. The Deputy Headmistress is the Designated Safeguarding Lead (DSL).

AIMS OF THE POLICY

Broadhurst School has a commitment to keeping children safe and healthy and protected from potential and known risks. The online safety policy operates under the umbrella of the Safeguarding Policy. The influence and value of ICT should be firmly embedded within the EYFS curriculum and it must therefore be reflected in practice. The following policy is in place to help modify behaviour and to promote the acceptable use of online technologies.

It is our aim to establish a culture which ensures the safety and well-being of children, this includes their online safety, and which also safeguards all staff members by encouraging them to work safely and responsibly and to monitor their own behaviours, standards and practice.

Developmentally appropriate access to computers and the internet in the early years contributes significantly to children's enjoyment of learning and development. Locked down and banning practices do not provide effective safeguards as prohibiting access to online technology can give a false sense of security. Children have rights as learners and should be entitled to have

access to appropriate technologies, they need to be empowered with the knowledge and skills to keep safe online.

This policy aims to promote awareness and provide information and support to parents/carers and staff.

PART 1: ROLES AND RESPONSIBILITIES

PROPIETOR
The proprietor has overall strategic responsibility for online safety within the school.

HEADMISTRESS
The Headmistress has ultimate responsibility for online 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 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 children who are in breach of acceptable use policies and responding to serious incidents involving online safety

DESIGNATED SAFEGUARDING LEAD
Where any online incident has serious implications for the child's safety or well-being, the matter should be referred to the DSL, who is the Deputy Headmistress, who will decide whether or not a referral should be made to Family Services and Social Work or the Police.

ONLINE SAFETY COORDINATOR
The Deputy Headmistress, who is also the Designated Safeguarding Lead (DSL), is the School's Online Safety Coordinator.

The Online Safety Coordinator will:

- monitor and review the school's online safety policy
- ensure that staff are aware that any online safety incident should be reported to the Online Safety Coordinator
- maintain a log of internet related incidents and co-ordinate any investigation into breaches, reporting any online safety incidents to Child Exploitation and Online Protection (CEOP) on 0870 000 3344 and Camden's Online Safety Coordinator
- ensure online safety is inclusive of children with special educational needs and disabilities (SEND)
- ensure that all staff have read and signed the Acceptable Use Agreement as part of their induction. (Appendix 4)
- provide the first point of contact and advice for school staff, children and parents
- liaise with the Headmistress to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature

NETWORK MANAGER - PERSON RESPONSIBLE FOR IT

The person in charge of IT will:

- carry out monitoring and audits of networks and report breaches to the Online Safety Coordinator or Headmistress
- support any subsequent investigation into breaches and preserving any evidence
- Ensure our IT system's security and virus protection are reviewed and updated regularly, to include a secure, filtered, managed internet service and broadband provider

TEACHERS AND TEACHING ASSISTANTS

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

- adhere to the school's online and acceptable use policy and procedures
- sign and return an Acceptable User Agreement (AUA) as part of their induction
- keep children safe when teaching or learning involves use of the internet, including for children with SEND
- plan use of the internet for lessons and research online materials and resources prior to their implementation or presentation to children
- report breaches of internet use to the Online Safety Coordinator
- recognise when children, including those with SEND, are at risk from their internet use or have had negative experiences and take appropriate action, for example, referral to the Online Safety Coordinator

Staff are always expected to follow the guidelines below:

- IT equipment belonging to Broadhurst School should never be used to access inappropriate material, such as obscene, hateful, pornographic or otherwise illegal material.
- Personal equipment containing inappropriate material should not be brought into school.
- Staff are aware of the risks of fostering online relationships with parents and children.
- Staff uphold their responsibility of confidentiality, inside and outside working hours.
- Staff take responsibility for their digital footprint (a trail of data created whilst using the internet), and that the use of social networking sites (such as Facebook, Twitter, Instagram) in staff recreational time on their own devices must not compromise professional integrity or bring the school into disrepute.
- Adding parents as 'friends' on social network sites or using their personal IT equipment, i.e. smart phone or tablet, to communicate with parents is against school policy
- Staff are aware of the risk from computer viruses, and opening emails from unknown sources.
- Any accessible computer should always be locked when unattended. This includes brief periods away from the computer, even when the room is empty.
- Our secure filtered internet server is used to monitor and prevent offensive material or spam. If, on a rare occasion, security systems are not able to identify and remove such materials, the material should be minimised from the desktop and the incident reported to the Online Safety Coordinator immediately.
- Computers should be placed in areas of high visibility which will enable children and adults to be closely supervised and their online use to be appropriately monitored.
- Children should only be able to access age-appropriate websites with adult supervision.
- No child should ever be left unsupervised whilst using any IT equipment.
- Children do not have access to social media in school.

PARENTS AND CARERS

The school realises the importance of involving parents and carers in the development and implementation of online safety strategies and policies. Most children will have internet access at home and out of school, including via their 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. It is therefore advantageous to consult and discuss emerging online safety issues with parents and carers. (Appendix 2)

Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. However, it should be supervised, and parents should be aware that they are responsible for their child's use of Internet resources at home.

This policy is available to parents on the school's website informing them of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

The Camden Safeguarding Children Partnership (CSCP) online safety leaflet for parents is available on the CSCP website: https://cscp.org.uk/parents-and-carers/online-safety/ Please see safeguarding policy for relevant contact numbers.

We have developed an Acceptable Use Agreement (AUA) which details the ways in which the internet can and cannot be used in School. (Appendix 5) We are responsible for the safety of children in our care but also for the behaviours and expectations of any adults who affect or come into contact with the school. All staff must read and sign their agreement.

Training sessions for staff regarding online safety are held when deemed suitable to renew by management.

PART 2: PROCEDURES

FILTERING AND MONITORING THE SYSTEM

- the DSL is responsible for online safety and works closely with the school's IT technician to appropriately monitor usage.
- the IT Technician is responsible for maintaining filtering and monitoring systems, generating reports and completing any actions following concerns.
- the DSL, Senior Leadership and school's IT Technician will review the filtering and monitoring provision at least annually.
- filtering procedures will block harmful content and will be appropriate to the needs of the school. Filtering will be appropriate but not restrictive and will not unreasonably impact or hinder learning.
- the DSL will monitor internet searches and usage frequently, this will be done by both physically monitoring school devices and an inspection of internet user logs. This action will be supported by the IT Technician.
- The DSL will follow up on any safeguarding concerns that may arise during the monitoring process.
- A risk assessment for filtering and monitoring procedures will be completed at least annually.

- access to the school internet system should be via individual logins and passwords for staff wherever possible.
- visitors, such as school inspectors, should have permission from the Headmistress or Online Safety Co-ordinator to access the system and be given a separate visitor log-in
- the Network Manager should keep a record of all logins used within the school for the purposes of monitoring and auditing internet activity.
- the online safety co-ordinator and teaching staff should carefully consider the location of internet-enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of children, in accordance with their age and experience.

CONFIDENTIALITY AND DATA PROTECTION

The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 1998. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.

A child's data that is being sent to other organisations will be sent via the school's secure system, ISAMS. Any breaches of data security should be reported to the Headmistress 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.

In the event that we need to move learning online, we use the platform Google Classroom, this is an extension of the classroom. We do not upload any personal information on Google Classroom and parents are only able to see information related to their child. The parents have dedicated access and can choose how to share any information or pictures from home. The Online Safety Coordinator has administration access on Google Classroom and can see everything that has been uploaded. The platform can be accessed online but only by those with login permissions. Our Acceptable Use Agreement states that accessors agree not to disseminate any information to third parties, to work in line with our Confidentiality and Sharing of Information Policy.

ACCEPTABLE USER AGREEMENTS

All internet users within the school will be expected to sign an acceptable use agreement, at induction, that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.

For any Reception age children, an Acceptable Use Agreement will be signed by parents on their child's behalf. This includes consent for their child to view material or play educational age-appropriate games via the internet in school. (Appendix 4)

Acceptable Use Agreements, signed using DocuSign, will be kept on ISAMS.

CURRICULUM

Online safety and relationships is part of Relationships, Sex and Health Education which is embedded into the school's Personal, Social and Emotional Development Curriculum.

Overall responsibility for the design and co-ordination of online safety education lies with the Headmistress and the Online Safety Co-ordinator, but all staff should play a role in delivering ongoing online safety education in the classroom as part of the curriculum. Teachers may wish to use Circle Time as a forum for discussion on online safety issues to ensure that children understand that there are some risks whilst online.

Rules regarding safe internet use should be displayed in all classrooms where computers are used to deliver lessons (Appendix 8).
Teachers should be aware of those children who may be more vulnerable to risk from internet use. These may include children with SEND or children with a high level of exposure to IT devises at home.

STAFF CONDUCT
School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with children. All school staff are in a position of trust and should act in a professional manner at all times.

Here is some key advice for staff to help protect their online reputation. The following points should 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 children should only be taken by staff in connection with educational purposes, for example, EYFS developmental learning journey or school trips
- staff should always use school equipment and only store images on the school computer system
- staff should take care regarding the content of and access to their own social networking sites and ensure that children and parents cannot gain access to these
- staff should ensure they understand the school's policies on the use of social media
- staff should not leave a computer or any other device logged on when away from their desk
- familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. (Appendix 3)
- it is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Center's Reputation mini site has more information on this
- be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos
- consider your own conduct online; certain behaviour could breach your employment code of conduct
- discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place
- Be aware that your social media friends may also be friends with children and their family members and therefore could read your post if you do not have appropriate privacy settings

- do not give out personal contact details – if children or parents need to contact you always use your school's contact details. On school trips, staff will have a school mobile for their use
- use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube
- staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal
- staff should 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 should not post any comments about specific children or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute
- staff should ensure that personal data relating to children is stored securely and encrypted if taken off the school premises
- where staff are using mobile equipment such as laptops or iPads provided by the school, they should ensure that the equipment is kept safe and secure at all times

STAFF TRAINING
All school staff should receive training with regard to IT systems and online safety as part of their induction.

School management should ensure that staff update training, as appropriate, in order to ensure they keep up to date with new developments in technology and any emerging safety issues and are aware of the risks and actions to take to keep children safe online.

'Parent Zone' has established a training programme designed to enable schools and professionals working with parents to deliver their own sessions on internet safety.

EXIT STRATEGY
When staff leave, any school equipment is returned. Pin numbers, passwords and other access codes are reset so that the staff member can be removed from the school's IT system. Any online accounts, such as Twinkl, are disabled and email accounts are closed.

INTERNET AND SEARCH ENGINES
- when using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk
- our children should be supervised at all times when using the internet
- All use of the internet should have a clearly defined educational purpose
- despite filtering systems, it is still possible for children to inadvertently access unsuitable websites. To reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information offline where possible

SAFE USE OF APPLICATIONS

- The school email system is hosted by an email system that allows content to be filtered.
- Individual email addresses for staff or children should not be published on the school website.
- Staff should be aware that use of the school internet system is for the purposes of education or school business only, and its use may be monitored

SCHOOL WEBSITE

- content should not be uploaded onto the school website unless it has been authorised by the Headmistress, who is responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law
- the school should designate a named person or persons to have responsibility for uploading materials onto the website. This is particularly important if the school allows a number of staff members to upload information onto the website
- to ensure the privacy and security of staff and children, the contact details on the website should be the school address, email and telephone number
- 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

PHOTOGRAPHIC AND VIDEO IMAGES

- where the school uses photographs and videos of children for publicity purposes, for example on the school website, images should be carefully selected so that individual children cannot be easily identified.
- where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear
- children's names should never be published where their photograph or video is being used
- staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images
- images should be securely stored only on the school's computer system and all other copies deleted
- staff must not use personal devices to take photographs of children
- schools should inform 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

CYBERBULLYING

Cyberbullying includes:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll

- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations

We seek to protect staff from cyberbullying by children, parents and other members of staff and supporting them if it happens.

- staff should never respond or retaliate to cyberbullying incidents. Staff should report incidents appropriately and seek support from a senior member of staff
- save evidence of the abuse; take screen prints of messages or web pages and record the time and date
- where the perpetrator is known to be a colleague, the majority of cases can be dealt with most effectively through the school's disciplinary procedures
- If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure they understand why the material is unacceptable or offensive and request they remove it. It is the School's responsibility to ensure this is reported.
- Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report. (Appendix 6)
- Guidance may be sought from the local authority, legal advisers or from other agencies, for example, The UK Safer Internet Centre
- Before you contact a service provider, it is important to be clear about where the content is; for example by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected of being illegal you should contact the police directly.
- Any comments that are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, staff or a representative from the school may consider contacting the local police. Online harassment is a crime

Employers have a duty to support staff and no one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if they are a member. The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the online issues, which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

REPORTING AND RESPONDING TO INCIDENTS

- 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 children or staff, must be recorded by the online safety co-ordinator on the online safety incident report form. (Appendix 7)

- A copy of the Online Safety Incident Report Form should be emailed to Camden Safeguarding Children Partnership at cscp@camden.gov.uk
- where the incident or complaint relates to a member of staff, the matter must always be referred to the Headmistress for action and consideration given to contacting the LADO where this is appropriate. Incidents involving the Headmistress should be reported to the Proprietor.
- the school's Online Safety Co-ordinator should keep a log of all online safety incidents and complaints ad 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 Camden Safeguarding Children Partnership

Although it is intended that online safety strategies and polices should reduce the risk to children whilst on-line, this cannot completely rule out the possibility that children 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 online learning environment.

UNINTENTIONAL ACCESS OF INAPPROPRIATE WEBSITES

- if a Child or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the children' age, teachers should immediately (and calmly) close or minimise the screen
- teachers should reassure children 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 coordinator and details of the website address and URL provided
- the online safety coordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate

INAPPROPRIATE USE OF IT BY STAFF

- if a member of staff witnesses misuse of IT by a colleague, they should report this to the Headmistress and the online safety co-ordinator immediately. If the misconduct involves the Headmistress, the matter should be reported to the Proprietor
- the online safety co-ordinator will notify the network manager 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 online safety co-ordinator will arrange with the network manager 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 Headmistress will take any necessary disciplinary action against the staff member and report the matter to the Proprietor 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 Headmistress or Proprietor should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form

RISK FROM CONTACT WITH VIOLENT EXTREMISTS

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 the 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. The contact for Broadhurst School is the Channel Panel, Camden.

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.

- staff need to be aware of the school's duty under the Prevent programme and be able to recognise any child who is being targeted by violent extremists via the internet for the purposes of radicalisation. Staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policy
- Children are taught the importance of being supervised when online for their own safety. (Appendix 4)
- the school should ensure that adequate filtering is in place and review filtering in response to any incident where a child or staff member accesses websites advocating violent extremism
- all incidents should be dealt with as a breach of the acceptable use agreements
- The school's behaviour and staff disciplinary procedures should be used as appropriate.
- the Online Safety Co-ordinator and the Designated Safeguarding Lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and review current school procedures to ensure they are robust enough to deal with the issue
- where there are concerns that a
    a. child is being radicalised
    b. child is in contact with violent extremists
    c. child's parents are being radicalised
    d. child's parents are in contact with violent extremist

  and this is placing the child or young person at risk, the school should refer the young person to the Channel Panel Camden

Further information is available from Camden Safeguarding Children Partnership at: https://cscp.org.uk/resources/radicalisation-and-extremism-resources/

Headmistress:		**Date:**	

APPENDIX 1

THE RISKS AND DANGERS OF BEING ONLINE

Inappropriate content, including pornography

Children and young people may see illegal or unsuitable content online, such as:

- pornography
- child abuse images
- dangerous advice encouraging eating disorders, self-harm or suicide
- excessive violence or race hate materials, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.
- Some websites show illegal content. Others that are legal might have unregulated advice or are meant for adults only. Children may come across this content by mistake.

Ignoring age restrictions

- age limits are in place to keep children safe; parents and carers should not feel pressurised into letting younger children join these websites

Friending or communicating with people they don't know

- children and young people may chat or become 'friends' with people on social networks or online games, even if they don't know them or have never met them in person. This makes children vulnerable to bullying, grooming and sharing personal information. It is imperative that parent/carers ensure that parental controls are activated on the electronic devices their children use.

Grooming and sexual abuse

- grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking
- children and young people can be groomed online or face-to-face, by a stranger or by someone they know - for example a family member, friend or professional
- groomers may be male or female and could be of any age
- many children and young people do not understand that they have been groomed or that what has happened is abuse

Signs of grooming

The signs of grooming are not always obvious and groomers will often go to great lengths not to be identified. If a child is being groomed they may:

- be very secretive, including about what they are doing online
- have older boyfriends or girlfriends

- have new things such as toys that they cannot or will not explain
- have access to drugs and alcohol through carers or older siblings and their friends

Grooming happens both online and in person. Groomers will hide their true intentions and may spend a long time gaining a child's trust. Groomers may try to gain the trust of a whole family to allow them to be left alone with a child and if they work with children they may use similar tactics with their colleagues.

Groomers do this by:

- pretending to be someone they are not
- offering advice or understanding
- buying gifts
- giving the child attention
- using their professional position or reputation
- taking them on trips, outings or holidays

Sharing personal information

Privacy controls can limit who can see your child's details, like their name, age and where they live.

Switch off or adjust settings using GPS or location tracking

Lots of apps and social networking sites use software to locate where the user is. Parent/carers need to ensure these are switched off.

APPENDIX 2

PARENTAL ADVICE

Parents should decide with their child the rules for using the Internet and decide together when, how long, and what comprises appropriate use.

Parents should get to know the sites their child visits and talk to them about what they are learning.

Parents should encourage their child not to respond to any uninvited messages and to tell them if they receive any such messages or images.

The Online Safety and Acceptable User Policy informs parents of online safety issues and advises them in reinforcing online safety messages at home. It also informs parents of their child's level of internet use within the school.

Parents may contact the school's Online Safety Co-ordinator if they have any concerns about their child's use of technology.

Free advice for parents is available from the following sources**:**

NSPCC- Keeping children safe online.

Website; https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Block'em is a free app for Android users that blocks unwanted calls and text messages from specified numbers. Their website also provides advice for iPhone users.

The Diana Award also runs a whole school Anti-Bullying Programme, information and good practice can be found at www.antibullyingpro.com.

APPENDIX 3

SAFE USE OF ONLINE SITES

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. Generally, these would have limited use in schools but children may have access to or experience of these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas online. Some schools may feel that these have an educational value.

Chat rooms are internet sites where users can join in 'conversations' online; **instant messaging** allows instant communications between two people online. The School internet system does host these applications.

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. The School internet system does not allow access to such sites.

These may not always apply to our age children but the School is aware in case parents ask for advice.

APPENDIX 4

Acceptable Use Agreement for Nursery Children

Name:

Class:

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

- I will ask a teacher if I want to use the computer/tablet/interactive touch screen
- I will only use activities that a teacher 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 if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I will tell a teacher if something online makes me feel unhappy or worried
- I know that if I break the rules, I might not be allowed to use a computer/tablet/interactive touch screen

Parents

I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school.

I understand that the school will take all reasonable precaution to ensure children do not have access to inappropriate websites, and that the school cannot be held responsible if children do not access inappropriate websites.

I agree that my child's work can be published on the school website.

Name:

Signed:

Date:

APPENDIX 5

Acceptable Use Agreement for Staff and Advisors

Access and Professional Use

- all computer networks and systems belong to the school and are made available to staff for educational, professional, administrative and governance purposes only
- staff are expected to abide by all school online rules and the terms of this acceptable use agreement. Failure to do so may result in disciplinary action being taken against staff
- the school reserves the right to monitor internet activity and examine and delete files from the school's system
- staff have a responsibility to safeguard children in their use of the internet and reporting all online concerns to the Headmistress
- copyright and intellectual property rights in relation to materials used from the internet must be respected
- emails and other written communications must be carefully written and polite in tone and nature
- anonymous messages and the forwarding of chain letters are not permitted
- staff will have access to the internet as agreed by the school
- staff will follow good practice advice at all times and will ensure online activity meets the standards expected of professional conduct

Data protection and system security

- staff and advisors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand
- use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented
- downloading executable files or unapproved system utilities will not be allowed and all files held on the school system will be regularly checked
- staff will not allow others to access their individual accounts
- sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log out when they have finished using a computer terminal
- files should be saved, stored and deleted in line with the school policy
- care will be taken to check copyright and not publish or distribute others' work without seeking permission

Personal use

- staff should not browse, download or send material that could be considered offensive to colleagues and children or is illegal
- staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe
- staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the School's name into disrepute
- school systems may not be used for private purposes without permission from the Headmistress
- use of school systems for financial gain, gambling, political purposes or advertising is not permitted

I have read the above policy and agree to abide by its terms.

Name: Date:
Signed:

APPENDIX 6

Contact details for social networking sites

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools.

Social networking site	Useful links
Ask.fm	Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.
BBM	Read BBM rules and safety
Facebook	Read Facebook's rules Report to Facebook Facebook Safety Centre
Instagram	Read Instagram's rules Report to Instagram Instagram Safety Centre
Kik Messenger	Read Kik's rules Report to Kik Kik Help Centre
Snapchat	Read Snapchat rules Report to Snapchat Read Snapchat's safety tips for parents
Tumblr	Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email
Twitter	Read Twitter's rules Report to Twitter
Vine	Read Vine's rules Contacting Vine and reporting
YouTube	Read YouTube's rules Report to YouTube YouTube Safety Centre

APPENDIX 7

Online Safety Incident Report Form

This form should be kept on file and a copy emailed to Camden Safeguarding Children Partnership at cscp@camden.gov.uk

School's details:

Name of school:

Address:

Name of Online Safety Coordinator:

Contact Details:

Details of incident

Date of Incident:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

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

Who was involved in the incident?
□ child □ 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 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 (i.e.: 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

Appendix 8- Classroom Online Safety Poster.