Wildwood

Nature School

Online Safety Policy

Purpose of the policy

This policy outlines Wildwood Nature School's strategy for safeguarding children against the risks involved in online technology and how we teach our children about how to keep safe online.

Contents

Key contacts

Co-head of school
Name: Tara Royle
Contact details: info@wildwoodnatureschool.org.uk

Online Safety Lead:
Name: Clare Bunston
Contact details:

Designated safeguarding lead:
Name: Clare Bunston
Contact details:

Nominated trustee:
Name:
Contact details:

London Borough of Camden

Child protection service manager and Local Authority Designated Officer (LADO):
Name: Jacqueline Fearon
Tel: 020 7974 4556
Email: LADO@camden.gov.uk

Child and Family Contact/MASH team:
Manager: Noella Hacquard
Tel: 020 7974 1553/3317
Email:LBCMASHadmin@camden.gov.uk

Camden online safety officer:
Name: Jenni Spencer
Tel: 020 7974 2866
Email: Jenni.spencer@camden.gov.uk

Prevent Education Officer
Name: Jane Murphy
Tel: 020 7974 1008
Email: Jane.murphy@camden.gov.uk

1. Introduction

At Wildwood Nature School, a key value and essential part of our ethos is that children develop a deep connection with nature by spending lots of time outdoors. However, we also recognise that children need to learn to be able to use the internet effectively and safely to succeed in tomorrow's world. Furthermore, the educational advantages of computing need to be harnessed to enhance children's learning.

This policy will address the risks associated with online use by children, as well as how we teach and ensure online safety for our children, staff and family community. Computing covers a wide range of activities, including access to information, electronic communications and social networking. Computing will be approached as a skill set to be learned that supports the children's learning in other areas. Wildwood Nature School balances the need to learn this skill set with our commitment to spending the majority of children's learning time outdoors in nature.

2. Risks associated with internet technology

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

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.

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 5.5 of this policy.

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.

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 5.5 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.

3. School online safety strategies

3.1 Whole school approach

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

We do this in a range of ways:

- Staff are 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 should be aware of the use of technology in child-on-child abuse;

- We consider online safety within other policy areas, such as staff conduct and anti-bullying;

- We ensure that consistent messages are given to staff and children and that everyone understands the online safety policy: staff receive suitable training around online safety and similar messages are taught to the children;

- Staff are aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with children, and schools must ensure there are clear policies available to staff on expectations for online behaviour.

- Our online safety policy is reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

- We use a dedicated education-tailored, web-filtering service (Netsweeper) which monitors all internet traffic into the school and blocks access to unsuitable content, and provides anti-virus/malware protection and monitoring systems

- Children are not permitted to use any device connected to the internet when away from the hall (as the web filtering will not be adequate), except wit 1:1 supervision from a teacher;

- We have a culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of online behaviour;

- Children are ***taught to keep themselves and others safe*** online and use technology responsibly; this is achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

Additional references:

DfE non-statutory guidance on teaching online safety

DfE statutory guidance on RSE

3.2 Roles and responsibilities

Wildwood Nature School's online safety strategy is inclusive of the whole school community, including children, staff, trustees, parents and carers.

3.2.1 Co-head of school's role

The co-head of school has 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 trustees 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 how to deal with staff and children who are in breach of acceptable use policies and responding to serious incidents involving online safety.

3.2.2 Trustees' role

Wildwood Nature School's trustees have a statutory responsibility for pupil safety. They are always kept informed of any online safety issues. The trustees have helped to create this policy and the school's online safety strategy and procedures and ensure that these are reviewed regularly.

Trustees regularly monitor and review our IT filtering systems to check their effectiveness and ensure that the leadership team is aware of what provision is in place and how to escalate any concerns.

Trustees are subject to the same online safety rules as staff members and, upon accepting their role as trustee, sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, trustees should always use business email addresses when conducting school business.

3.2.3 Online Safety Lead's role

Wildwood Nature School's Online Safety Lead is responsible for coordinating online safety policies on behalf of the school.

The Online Safety Lead 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 children 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, trustees, children and parents;
- liaise with the co-head of school and nominated trustee 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 children have read and signed the acceptable use policy (AUP);
- report annually to the board of trustees 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.

The Online Safety Lead receives recognised training in order to carry out their role more effectively.

3.2.4 Role of school staff

All school staff at Wildwood Nature School have a dual role concerning their own internet use and providing guidance, support and supervision for children. 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 children;
- keeping children safe and ensuring they receive appropriate supervision and support whilst using the internet;
- planning use of the internet for lessons and researching online materials and resources;
- reporting breaches of internet use to the Online Safety Lead;
- recognising when children are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the Online Safety Lead;
- ensuring that the online safety and digital literacy elements of the curriculum are effectively taught.

3.2.5 Designated safeguarding lead

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 (DSL) for the school who will decide whether or not a referral should be made to Children's Safeguarding and Social Work or the Police.

3.3 Children with special educational needs and disabilities (SEND)

Children 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. At Wildwood Nature School, we have a flexible and personalised approach to online safeguarding for these children in order to meet their needs.

The SEND Lead is responsible for providing extra support for these children and does this by:

- linking with the Online Safety Lead to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for children with SEND;
- where necessary, liaising with the Online Safety Lead 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 children with SEND;
- ensuring that the school's online safety policy is adapted to suit the needs of children with SEND;
- maintaining awareness that some children with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences;

- liaising with parents, carers and other relevant agencies in developing online safety practices for children with SEND;
- keeping up to date with any developments regarding emerging technologies and online safety and how these may impact on children with SEND.

3.4 Working with parents and carers

Given how important our family community is at Wildwood Nature School, we prioritise the involvement of parents and carers in the development and implementation of our 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.

We offer online safety training opportunities to parents in order to provide them with information to help them keep their child safe online. In the first instance, we direct them to the CSCP online safety leaflet for parents:
https://cscp.org.uk/parents-and-carers/online-safety/

The co-head of school, board of trustees and the Online Safety Lead regularly consider what strategies to adopt in order to ensure parents are aware of online safety issues and how to support them in reinforcing online safety messages at home.

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 are also informed that they can contact the school's Online Safety Lead if they have any concerns about their child's use of technology.

Where remote online learning is being used, parents are made aware of what arrangements have been made, which websites children will be accessing and any member of staff they will be interacting with online.

4. Online safety policies

4.1 Accessing and monitoring the system

- Access to the school internet system is via individual log-ins and passwords for staff and children. Visitors are given permission from the co-head of school or Online

Safety Lead to access the system and be given a separate visitors log-in.

- The Online Safety Lead keeps a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- Staff are required to change their password every 6 months.

- The Online Safety Lead and teaching staff carefully consider the location of internet enabled devices in the teaching areas in order to allow an appropriate level of supervision of children depending on their age and experience.

4.2 Confidentiality and data protection

- Wildwood Nature 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. Any breaches of data security should be reported to the co-head of school immediately.

- The school uses security cameras at the entrance as part of the premises security measures. A notice is 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 will be expected to sign an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.

- Acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet in school (see Appendix 1).

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see Appendix 2).

The school's Online Safety Lead will keep a copy of all signed acceptable use agreements.

4.4 Teaching online safety

3.4.1 Responsibility

One of the key features of the Wildwood Nature School's online safety strategy is teaching children to protect themselves and behave responsibly while online. There is an expectation that over time, children will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the co-head of school and the Online Safety Lead, but all staff should play a role in delivering online safety messages.

- The Online Safety Lead 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 as part of the curriculum.

- Rules regarding safe internet use are posted up near the computers.

- The start of every lesson where computers are being used should be an opportunity to remind children of expectations on internet use and the need to follow basic principles in order to keep safe.

- We are required to teach about online bullying as part of statutory Relationships Education and health education.

- Well-being lessons provide an ideal opportunity for discussion on online safety issues to ensure that children understand the risks and why it is important to regulate their behaviour whilst on-line.

- Teachers should be 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 children with SEND.

- Teachers should ensure that the school's policy on children' use of their own mobile phones and other mobile devices in school is adhered to.

4.4.2 Content

Children 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 evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems;
- are responsible, competent, confident and creative users of information and communication technology.

The children at Wildwood Nature School are taught all elements of online safety included in Statutory Relationships Education:

- 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.

Our well-being curriculum includes the following elements from the Statutory Health Education:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental well-being;
- 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 well-being;
- 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.

4.5 Staff training and conduct

4.5.1 Training

- All school staff and trustees should receive training with regard to IT systems and online safety as part of their induction and this should include a meeting with the Online Safety Lead.

- Staff should also attend specific training on online safety so that they are aware of the risks and actions to take to keep children safe online. School management ensures that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

4.5.2 IT and safe teaching practice

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. Staff should refer to the model social media policy for school staff for further guidance.
Schools and Nurseries Safeguarding Policies - Camden Safeguarding Children Partnership — CSCP

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, such as to record their work on Tapestry Journal or for school trips.

- Staff should 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 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 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 not engage in any conversation with children via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with children regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or children 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 children.

- When making contact with parents or children by email, staff should always use their school email address or account. Personal email addresses and accounts should never be used.

- 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 tablets provided by the school, they should ensure that the equipment is kept safe and secure at all times.

4.5.3 Exit strategy

When staff leave, their line manager should liaise with the Online Safety Lead to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes be reset so that the staff member can be removed from the school's IT system.

4.6 Safe use of technology

4.6.1 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 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 children 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 Lead, who will liaise with the IT service provider for temporary access. Teachers should notify the Online Safety Lead once access is no longer needed to ensure the site is blocked.

4.6.2 Evaluating and using internet content

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

4.6.3 Safe use of applications

The school email system is hosted by an email system that allows content to be filtered and allows children 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. Generally, these would have limited use in schools but children 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. Some schools may feel that these have an educational value.

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, children will use these at home and are rarely used at school.

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 the school internet system.

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 children from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- At times, a member of staff may identify a clear educational use for emails or social networking sites and forums for on-line publishing, and will only use approved sites such as those provided by the IT service provider. Any use of these sites are 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 children in connection with school business must be checked and cleared by the responsible teacher.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the Online Safety Lead who will liaise with the learning platform provider.

- Apart from the co-head of school, individual email addresses for staff or children are not published on the school website.

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

- Children 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 should be polite; if a child receives an offensive or distressing email or comment, they are instructed not to reply and to notify the responsible teacher immediately.

- Children should be 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 should be aware that the use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

- In order to teach children to stay safe online outside of school, they are advised:

  - not to give out personal details to anyone online 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 online 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 online that may help to identify or locate them or anyone else;
- not to arrange to meet anyone whom they have only met online or go "off-line" with anyone they meet in a chat room;
- to behave responsibly whilst online 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.

4.6.4 Video calling and remote learning

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

In the event that Wildwood Nature School needs to conduct remote learning, we will ensure online safety by:

- only using school registered accounts rather than personal accounts;
- recording remote learning for safeguarding purposes;
- ensuring the security of the video link;
- checking settings regularly to ensure teachers have full control of the meeting i.e.; 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://www.lgfl.net/online-safety/ https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

4.6.5 School website

- Content is not uploaded onto the school website unless it has been authorised by the Online Safety Lead and the co-head of school, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- To ensure the privacy and security of staff and children, the contact details on the website are the school address, email and telephone number. No contact details for staff or children are displayed on the website.

- Children’s full names are never published on the website.

- Links to any external websites are regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

4.6.6 Photographic and video images

- When photographs and videos of children are used for Wildwood Nature School’s publicity purposes, images are 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 are never 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.

- Stored images should not be labelled with the child’s name and all images held of children are deleted once the child has left the school.

- Staff should not use personal devices to take photographs of children.

- We 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.

4.6.7 Children’s own mobile devices

The majority of children are likely to have mobile phones or other devices that allow them to access internet services, as many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. Since these can pose a major problem in that their use may distract children during lessons and may be used for online bullying, Wildwood Nature School does not allow children to keep their mobile phones with them during the school day. They are required to leave their mobile phones in a secure box in the school office. See our *Mobile Phone Policy*.

5. Responding to incidents

5.1 Policy statement

- All significant or complex incidents and complaints relating to online safety and unacceptable internet use will be reported to the Online Safety Lead in the first instance. All incidents, whether involving children or staff, must be recorded by the Online Safety Lead on the online safety incident report form (Appendix 3).

- 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 co-head of school 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 co-head of school should be reported to the chair of the board of trustees. Managing Allegations Against Staff and Volunteers & LADO - Camden Safeguarding Children Partnership — CSCP

- Our Online Safety Lead keeps a log of all online safety incidents and complaints and regularly reviews the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and uses these to update the online safety policy.

- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the DSL, 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 co-head of school.

Although it is intended that online safety strategies and policies should reduce the risk to children whilst online, 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 e-learning environment.

5.2 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 Lead and details of the website address and URL provided.

- The Online Safety Lead should liaise with the learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

5.3 Intentional access of inappropriate websites by a child

- If a child deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy (see section 6).

- The incident should be reported to the Online Safety Lead and details of the website address and URL recorded.

- The Online Safety Lead should liaise with the learning platform provider to ensure that access to the site is blocked.

- The child's parents should be notified of the incident and what action will be taken.

5.4 Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the co-head of school and the Online Safety Lead immediately. If the misconduct involves the co-head of school or trustee, the matter should be reported to the chair of the board of trustees.

- The Online Safety Lead will ensure 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 Lead will arrange with the learning platform provider 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 co-head of school will take any necessary disciplinary action against the staff member and report the matter to the school trustees 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 co-head of school or trustee should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.

5.5 Online bullying

5.5.1 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 children 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 children 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.

5.5.2 Dealing with incidents

The following covers all incidents of bullying that involve children at the school, whether or not they take place on school premises or outside school. All incidents should be dealt with under our *Behaviour Policy*, *Anti-Bullying Policy*, and the child-on-child abuse guidance. Schools and Nurseries Safeguarding Policies - Camden Safeguarding Children Partnership — CSCP

- Any incidents of online bullying should be reported to the Online Safety Lead 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 anti-bullying policies.

- 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, children should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.

- Children should be 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. In most instances, we will follow the procedures as outlined in our *Behaviour Policy* for conflict resolution and restorative justice. All incidents of bullying will be recorded in our *Bullying Log* as per our *Anti-Bullying Policy*.

5.5.3 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, the mobile phone company can be contacted to ask them to trace the calls. The child 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, contact the service provider so that the sender can be traced. The child should also consider changing email address.

- Where bullying takes place in chat rooms or gaming sites, the child 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, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

5.5.4 Online bullying of school staff

- School staff may become victims of online bullying by children and/or their parents. Because of the duty of care owed to staff, the co-head of school ensures that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against children and parents.

- Incidents of online bullying involving school staff should be recorded and monitored by the Online Safety Lead in the same manner as incidents involving children.

- Staff should follow the guidance on safe IT use in section 4.5.2 of this policy and avoid using their own mobile phones or email addresses to contact parents or children so that no record of these details becomes available.

- Personal contact details for staff are not posted on the school website or in any other school publication.

- Staff should follow the advice above on online bullying of children and not reply to messages but report the incident to the co-head of school immediately.

- Where the bullying is being carried out by parents the co-head of school should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.

5.6 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 sexual harassment or online bullying and because of the nature of online activities this can lead to more widespread harm and repeat victimisation.

Keeping children safe in education (2022) places a duty on schools to respond to any incidents of online sexual harassment such as:

- consensual and non-consensual sharing of nude and semi-nude images;
- sexualised online bullying;
- unwanted sexualised comments and messages;
- sexual exploitation, coercion or threats;
- coercing others into sharing images or performing acts online that they are not comfortable with.

Refer to the *Child on child abuse and sexual violence and harassment guidance for schools and colleges* for further details on what actions need to be taken in response to online sexual harassment. Schools and Nurseries Safeguarding Policies - Camden Safeguarding Children Partnership — CSCP

Wildwood Nature School makes children aware that producing and distributing sexual images to peers via the internet or mobile devices may be illegal. Children 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 be able 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

Wildwood Nature School is also aware that sometimes these behaviours may be linked to the sexual exploitation of a child or might be carried out as a gang-related activity. Staff should refer to the CSCP *Extra-familial harm and child exploitation guidance* for further details.

5.7 Risk from inappropriate contacts with adults

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

School staff should also be aware of children being 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 should be reported to the Online Safety Lead and the DSL.

- The DSL 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 DSL 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 child on how to terminate the contact and change contact details where necessary to ensure no further contact.

- The DSL and the Online Safety Lead should always notify the child's parents of any concerns or incidents and where appropriate, arrange to meet with them to 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 Lead should make a note of all actions taken and contact the 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 children is minimised.

5.8 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 need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Children and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- Wildwood Nature School ensures that adequate filtering is in place and reviews 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 policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.

- The Online Safety Lead and the DSL should 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, schools should refer the young person to the MASH. Guidance can be sought from the Prevent Education Manager.

Further information is available in the CSCP guidance *Safeguarding children and young people from radicalisation and extremism.*

5.9 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.

- Wildwood Nature School ensures that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of our well-being curriculum.

- Our key person system and regular 1:1 check-ins provide opportunities for chldren to discuss issues affecting them and to establish whether their online activities are an added risk factor.

- Staff receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

6. Responses to the misuse of school IT

In line with Wildwood Nature School's *Behaviour Policy*, we respond to all incidents and breaches of agreements in an individualised way, taking into consideration the child's circumstances and any unmet needs. All children have signed (via their parents) an acceptable use agreement. Any breaches of this agreement will be responded to because Wildwood Nature School recognises how important it is to keep everyone safe online. Below are 4 categories of infringements of the acceptable use agreement and examples of possible responses.

6.1 Responses for children

6.1.1 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.

Possible responses could include referral to the child's key person as well as a referral to the Online Safety Lead to talk about why we have online safety rules in place.

6.1.2 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.

Possible responses could include:

- referral to the child's key person
- referral to Online Safety Lead
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

6.1.3 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 others’ 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.

Possible responses could include:

- referral to child’s key person
- referral to Online Safety Lead
- referral to co-head of school
- loss of access to the internet for a period of time
- contact with parents.

6.1.4 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.

Possible responses could include:

- referral to co-head of school
- contact with parents
- removal of equipment
- referral to community police officer
- referral to Camden’s online safety officer.

6.2 Responses for staff

These 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. Responses are linked to the staff code of conduct.

6.2.1 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 co-head of school as a low level incident in line with the school's staff code of conduct.

- 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 children 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 responses include referral to the co-head of school who will issue a warning.

6.2.2 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. Managing Allegations Against Staff and Volunteers & LADO - Camden Safeguarding Children Partnership — CSCP

- 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 responses include:

- referral to the co-head of school
- removal of equipment
- referral to Camden’s online safety officer
- referral to Camden’s LADO or the police
- suspension pending investigation.

Policy review
Policy created: February 2023
Last reviewed:
Last modified: June 2023
Next review date: February 2025

Appendix 1

Acceptable use policy for primary school children

Name:
School:

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:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend
- only email people I know or if my teacher agrees
- only use my school email address
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.

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 precautions to ensure children do not have access to inappropriate websites, and that the school cannot be held responsible if children do access inappropriate websites.

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

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:
Date:

Appendix 2
Acceptable use policy for staff and trustees

Access and professional use

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

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

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

- Staff and trustees have a responsibility to safeguard children in their use of the internet and reporting all online safety concerns to the Online Safety Lead.

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

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

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

- Staff and trustees will have access to the internet as agreed by the school but will take care not to allow children to use their logon to search the internet.

- Staff and trustees 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 trustees 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 is permitted where virus checks can be implemented on the school ICT system.

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

- Staff and trustees 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 and trustees should not browse, download or send material that could be considered offensive to colleagues and children or is illegal.

- Staff and trustees 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 and trustees 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 ICT systems may not be used for private purposes without permission from the co-head of school.

- Use of school ICT 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:
School:
Signed:
Date:

Appendix 3
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 details

Name of school:

Address:

Name of Online Safety Lead:

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 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, transphobic, bi-phobic, religious hate material
□ terrorist material
□ Online grooming

□ Online radicalisation
□ Child abuse images
□ Online gambling
□ Softcore 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 co-head of school
□ 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:

Name:

Role:

Signed:

Date: