



Digital safety policy (including filtering and monitoring)



Shoreditch Park Primary School is a Rights Respecting School

School policies respect the UN convention on the rights of the child.

The Digital Safety and Filtering and Monitoring policy links to:

Article 13- every child must be free to express their thoughts and opinions and to access all kinds of information

Article 16- every child has the right to privacy

Article 17- every child has the right to reliable information...[and protection from] information which may be harmful.

1. Aims

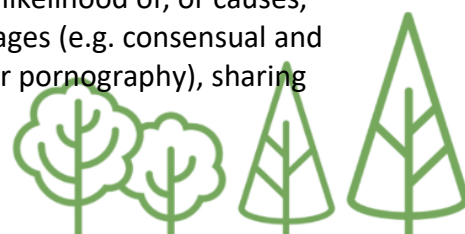
Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and



- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss



with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Leads

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSLs take responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place



- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4. Technical support staff (Classroom 365)

It is the responsibility of the school to ensure their technical support company and technicians carry out any E-Safety measures, and that they are aware of this policy.

Their role includes:

- Ensuring the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring the school meets the E-Safety technical requirements outlined by the LGfL and Local Authority guidance
- Ensuring users may only access the school's networks through a properly enforced password protection policy
- Ensuring LGfL is informed of issues relating to the filtering applied by theGrid
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files



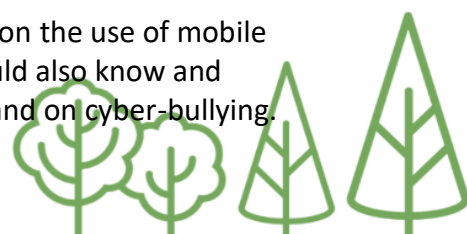
3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Digital communications with pupils should be on a professional level and only carried out using official school systems.
- Ensuring that digital safety is regularly discussed and that e-safety is embedded in all aspects of the curriculum and other school activities.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by immediately contacting a DSL.
- Following the correct procedures by completing a request form if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Monitoring ICT activity in lessons, extracurricular and extended school activities.
- They are aware of digital safety issues relating to the use of mobile phones, cameras and hand held devices and they monitor their use.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and follow the procedure in place for dealing with unsuitable material that is found in internet searches.

3.6. Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.



- Understand the importance of adopting good Digital Safety practice when using digital technologies out of school and realise that the school's Digital Safety Policy covers their actions out of school, if related to their membership of the school

3.7 Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents

and carers do not fully understand the issues and are less experienced in the use of ICT than their

children. The school will therefore take every opportunity to help parents understand these issues

through parents' evenings, newsletters, letters, website and information about national and local Online Safety campaigns.

Parents and carers will be responsible for:

- Endorsing (by signature) the Permissions Letter regarding their child's use of the internet and use of their child's images.
- Accessing the school website and any on-line pupil records in accordance with the relevant school Acceptable Use Policy.
- Notifying a member of staff or the Headteacher of any concerns or queries regarding this policy

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- 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

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

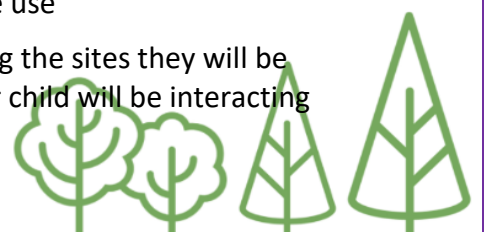
Please see the school website for the [computing curriculum map](#).

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety by holding regular workshops, adding safeguarding tips to the weekly newsletter and regularly updating the resources on the school website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online



If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with a DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Positive Behaviour and Anti-Bullying Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including through our ASPIRE lessons.

All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

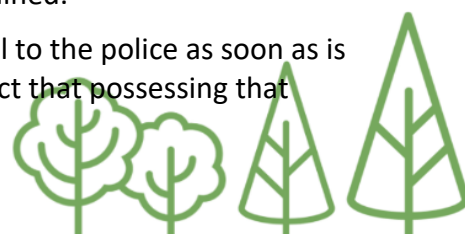
The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy:

- All complaints to go to the Class Teacher before reporting it to an appropriate staff member- either the Deputy Headteacher, Year Group Lead or a DSL.
- The member of school staff who is investigating the incident should establish the circumstances of the incident (s) by speaking to any adults or pupils who witnessed it. Records should be made of the content of the discussions.
- All staff will be aware of and directly challenge any racist, sexist homophobic/transphobic language. This is unacceptable in our school.
- School staff will involve parents and explain action taken, why and what they can do to reinforce and support.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that



material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Hackney MASH.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher and Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image



- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI) and cyberbullying

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Shoreditch Park Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Shoreditch Park Primary School will treat any use of AI to bully pupils in line with our Positive Behaviour and Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in the appendices.

8. Pupils using mobile devices in school

Children are not allowed to have mobile phones with them in school at any time. If pupils require a mobile phone in order to ensure they have a safe journey to and from school, they will be expected to lock their phones away in the designated lockers in the Year 5 and 6 Classrooms or in the school office.



9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, weekly bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
 - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.



Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Accessing the internet safely

11.1- Online safety procedures

Shoreditch Park Primary School:

- is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in areas where older pupils have more flexible access.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age or subject appropriate web sites
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where appropriate; eg kidrex, yahoo for kids or ask for kids.
- Is vigilant when conducting 'raw' image or internet searches with pupils e.g. Google image search Informs users that Internet use is monitored Informs staff and students that that they must report any failure of the filtering systems directly to the Filtering and Monitoring Team.
- Requires all staff to sign an Acceptable Use Form, and keeps a copy on file.
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the Permissions agreement form at time of their child's entry to the school.
- Makes clear all users know and understand what the rules of appropriate use are, and what sanctions result from misuse.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents Provides online safety advice for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities, e.g. the Police and/or the LA.

11.2- Procedures when unsuitable content has been viewed

Shoreditch Park Primary school fosters a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable either in or out of school.



At the start of every lesson involving ICT teachers will remind pupils what to do if they view content that makes them uncomfortable. Pupils know to either switch off their monitor, close the iPad screen or minimise their screen and report the concerning content to the teacher / supporting adult immediately.

Staff know to take a note of the time of the incident and/or the URL (depending on if pupils are able to view the screen) and to contact a DSL immediately.

12. Homework

Some pupils have homework set through Google Classrooms and IXL learning. To access this, every child will have a unique log in email address for which the email function has been disabled. In order to keep children safe, the following measures have been put in place:

- All comments boxes have been disabled to avoid inappropriate comments and constant moderation of forum.
- Video chat options to be disabled at all times.
- Children are to sign acceptable use policy and create an online safety class charter in class through Digital Safety lessons. In the event that a child breaches any of the agreements within the acceptable use policies, teachers will identify this and follow up with parents regarding appropriate communication.

13. Use of digital images

- Digital images /videos of pupils may be stored in a private teachers' shared images folder on the network and images should be deleted at the end of the year – unless an item is specifically kept for a key school publication.
- When using a staff or school iPad, pin codes must be used to keep all materials and images safe and secure.
- School mobile phones are provided for school trips. Photos can be taken on this device as they are password protected.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils

14. Website and social media

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website administrators The school web site complies with the school's guidelines for publications Most material is the school's own work.



- Where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address: admin@shoreditchpark.hackney.sch.uk
- Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

15. CCTV

CCTV We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

16. Filtering and monitoring

Shoreditch Park Primary School takes its responsibility to ensure effective filtering and monitoring seriously. The information below outlines our roles and responsibilities in relation to filtering and monitoring.

16.1. Who is responsible for filtering and monitoring at Shoreditch Park Primary School?

The key staff members involved in filtering and monitoring are:

Although the school has designated staff to lead on filtering and monitoring all staff play a part in ensuring that the school's filtering and monitoring systems are fit for purpose. The

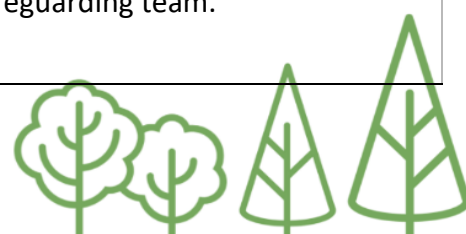
Filtering and monitoring lead	Nominated governor for filtering and monitoring	ICT Lead	IT provider
Claire Deegan	Caroline Doherty	Zeynep Karatay	Classroom 365

whole school has had training on filtering and monitoring and staff know that they play an important role in monitoring pupils' screens and reporting any inappropriate content to the safeguarding team.



16.2. What systems does Shoreditch Park have in place to ensure that effective monitoring systems are in place?

Are incidents urgently picked up, acted on and the outcomes recorded?	Staff monitor pupil screens to ensure that they are not accessing inappropriate content. Any attempts to access inappropriate content are flagged and shared with key staff members in reports from Classroom 365. We are looking at software that will immediately notify key staff members when attempts are made to access inappropriate content.
Are all staff clear on: • How to deal with these incidents • Who should lead on any actions	Yes- staff have had training on this.
How does the system meet the following principles:	
Age appropriate ○ Can you vary your strategy to take age, vulnerability, or specific situations into account	We can vary our systems according to vulnerability but generally only allow pupils to access content that is suitable for all.
Audit trail ○ Are any changes to the strategy logged so no one can make changes on their own?	Changes to strategy are logged and only the IT provider can make changes to the monitoring system.
Impact ○ How do monitoring results impact your policy and practice?	Through weekly audits of the school's filtering and monitoring systems any areas of concern are quickly addressed by the safeguarding team.



Bring your own device (BYOD) ○ If your system can monitor staff and pupils' personal devices, make sure this is done according to your data management policies. For example, will your system monitor devices out of school hours?	Pupils do not bring their own devices into school. Phones are locked up during the school day. Staff who use their personal phones during break times using the school wifi are aware that their internet usage will be monitored and that the filtering system will block certain content.
Is device monitoring managed? (this could be by your IT staff or a third-party provider) Whoever is managing device monitoring will need to: ● Make sure monitoring systems are working as expected ● Provide reports on pupil device activity ● Receive safeguarding training including online safety ● Record and report safeguarding concerns to the DSL	Our device monitoring is managed by Classroom 365 who check send monitoring reports and highlight safeguarding concerns to the DSLs. The school's SLT also runs weekly checks to ensure that the systems are working and keeps an audit trail of these checks.
Is your monitoring data received in a format that your staff can understand?	Yes- the reports we currently receive show the websites that have been accessed or attempted to be accessed.
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	We can identify IP addresses. KS1 pupils have named iPads. KS2 pupils login to laptops with their personal username. Pupil screens should always be monitored so there should be limited opportunities for them to access inappropriate content.
● Multiple language support ○ Can the system manage relevant languages to your school?	Yes- LGFL webprotect filters 46 languages.



● Reporting ○ How are alerts recorded and communicated?	If staff identify inappropriate content has been accessed they will record this in writing for DSLs, with URLs where possible. This is immediately shared with Classroom365 who will ensure that the website is blocked.
● Monitoring policy ○ How do you tell all users that you're monitoring their online access? ○ How do you communicate your expectations on appropriate use to pupils and staff?	Staff are aware that if they are online using the school wifi their online access is being monitored. Staff have had training on filtering and monitoring and been informed of expectations in the school bulletin. Pupils are reminded of the expectations when they are online at the start of every lesson involving technology. They are aware that the content they access is being monitored.
Do your staff: ● Provide effective supervision ● Take steps to maintain awareness of how devices are being used by pupils ● Report any safeguarding concerns to the DSL	Yes, staff have had training on this and are reminded of expectations in weekly safeguarding briefings. Teachers are expected to remind pupils that their activity is being monitored and how to report a concern at the start of every lesson involving ICT.

16.3 How do staff carry out weekly monitoring checks?

The school receives weekly reports from Classroom365 showing any content that the filtering systems has blocked.

The school's SLT also manually check a number of devices in different locations in the school to ensure that they meet the monitoring standards. This information is recorded in a monitoring log. Any actions are immediately highlighted to our IT provider Classroom365.



Software has been installed so that DSLs are alerted when there have been attempts to access inappropriate content.

16.4. How does the school carry out its annual filtering and monitoring review?

Shoreditch Park Primary School's annual filtering and monitoring review is conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review are recorded for reference and made available to those entitled to inspect that information.

The meeting covers:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what our filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements, for example, our RHSE and PSHE curriculum
- what related safeguarding or technology policies we have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review then informs:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review is carried out as a minimum annually but we may also hold a review when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

16.5. Who is our filtering provider and does it meet the standards set out in the government's [Filtering and Monitoring guidance](#)?



Shoreditch Park Primary School's filtering system is called Webscreen and is provided by LGFL. You can read LGFL's self-certification showing that the service meets the government standards here: <https://static.lgfl.net/lgflnet/downloads/online-safety/lgfl-os-appropriate-filtering-for-education-settings-provider-response-june-2016.pdf>

The table below sets out how Webscreen meets the filtering standards set out by the government.

Is it a member of the Internet Watch Foundation (IWF)?	Yes
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	Yes
Does it block access to illegal content including child sexual abuse material (CSAM)?	Yes
Are you satisfied that the system manages the following content: ● Discrimination ● Drugs/substance abuse ● Extremism ● Gambling ● Malware/hacking ● Pornography ● Piracy and copyright theft ● Self harm ● Violence	Yes
Is the filtering system: ● Operational ● Up to date ● Applied to all: ○ Users, including guest accounts ○ School-owned devices ○ Devices using the school broadband connection	Yes



Does the filtering system: ● Filter all internet feeds, including any backup connections ● Handle multilingual web content, images, common misspellings and abbreviations ● Identify technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and block them ● Provide alerts when any web content has been blocked It is: ● Age and ability appropriate for the users, and suitable for educational settings	Yes
Does the filtering system allow you to identify: ● Device name or ID, IP address, and where possible, the individual ● The time and date of attempted access ● The search term or content being blocked	Yes
Are you clear on how long logfile information (internet history) is retained and how it's stored?	Yes
Are you clear on how the system does not over block access so it doesn't lead to unreasonable restrictions?	Yes- staff can request for appropriate sites to be unblocked.



Does the filtering system meet the following principles? ● Context appropriate differentiated filtering, based on age, vulnerability and risk of harm ○ Can you vary the filtering strength? E.g. for staff? ● Circumvention ○ Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS) ● Control ○ Can you control the filter yourselves to permit or deny specific content? ○ Can you log any changes as part of an audit trail? ● Contextual content filters ○ In addition to URL or IP-based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter ● Filtering Policy ○ Does your provider detail its approach to filtering, as well as over blocking? ● Group/multi-site management ○ Can your system be deployed centrally, with a central policy and dashboard? ● Identification ○ Does the system allow you to identify users? ● Multiple language support ○ Does the system manage relevant languages? ● Network level ○ Is the filtering provided at 'network level', i.e. it doesn't rely on software on user devices while at school	Yes
---	------------



● Remote devices ○ Can the system filter devices where staff and/or pupils are working remotely? ● Reporting ○ Can you report inappropriate content? ○ Does the system provide clear historical information on the websites users have accessed or tried to access? ● Safe Search ○ Does the system have the ability to enforce 'safe search'?	Yes
If users access content via mobile or through apps: Get confirmation that your provider can provide filtering on mobile or app technologies. They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm.	Yes
If your filtering provision is procured with a broadband service: Make sure it meets the needs of your school or college	Yes

17. Policy monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

18. Links with other policies

This online safety policy is linked to our:

- [Child Protection and Safeguarding Policy](#)
- [Positive Behaviour and Anti-Bullying Policy](#)
- [Staff code of conduct](#)
- [Staff disciplinary procedures](#)



- [Parent/child acceptable use policy](#)



Appendix 1: staff, governor, visitor and volunteer acceptable use policy

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors (including supply staff)

Name of staff member/governor/volunteer/visitor:

This agreement covers the use of digital technologies in Shoreditch Park Primary including email, internet, shared network drives, network resources, all software, electronic equipment and all systems – inclusive of any iPad allocated to use for work purposes.

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school

- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I will only use Shoreditch Park Primary's digital technology resources and systems for professional purposes
- I will not reveal my password(s) to anyone
- I will ensure that any iPad allocated to me is protected by my login which is only shared with school administrators (subject lead and business manager) and remains on the school premises, unless written approval has been granted.
- I will follow 'best practice' advice in the creation and use of my password(s). If my password is compromised, I will ensure I change it
- I will not use anyone else's password, nor seek to discover it. If a colleague does reveal it to me, I will advise them to change it
- I will not allow unauthorized individuals to access any of Shoreditch Park Primary's systems
- I will ensure all documents and digital resources are saved, accessed and deleted in accordance with the Shoreditch Park Primary's network and data security and confidentiality protocols



- I will not engage in any online activity that compromises my professional responsibilities, code of conduct or professional boundaries
- My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods, even if they have recently left or no longer use the service
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to the Claire Deegan (Filtering and Monitoring Lead)
- I will not download any software or resources that can compromise the network, that breach a user's copyright, or are not correctly licensed
- I will not publish or distribute work that is protected by copyright
- I will not connect a computer, laptop, notebook or other electronic device (including USB flash drive) to the network that does not have up-to-date anti-virus software
- I will not use personal digital cameras or phones for taking and transferring images of children/young people or staff/volunteers without written permission, and will use those images only for their intended purpose
- I will ensure that any personal social networking sites/blogs, Twitter, Instagram accounts, etc., that I create or actively contribute to are separate from my professional role
- It is my responsibility to ensure that my use of social networking sites/blogs, etc., does not compromise my professional role, and will ensure my privacy settings are appropriate
- Using such sites in work, on mobile devices or school computers is prohibited
- Any computer, laptop or electronic device loaned to me by Shoreditch Park Primary is provided solely for professional use whilst under contract at Shoreditch park Primary School. Upon the termination of working contract, I understand that any equipment must be returned 30 days prior to my last working day. Failure to do so will result in the funds being recuperated in my final pay check.
- I will access Shoreditch Park Primary's resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those resources
- Any confidential data that I transport from one location to another will be protected by encryption
- I will follow Shoreditch Park Primary's data security protocols when using confidential data at any location
- Any information seen by me with regard to service users held within Shoreditch Park Primary will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority, e.g. Children's Social Care and/or the police
- It is my duty to support a whole organization safeguarding approach and I will alert the Shoreditch Park Primary's named child protection officer/relevant senior member of staff if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern
- It is my responsibility to ensure that I remain up-to-date, read and understand the Shoreditch Park Primary's most recent online safety policies
- I understand that all internet, network and location services (MDM Software) usage are logged and this information can be made available to SLT upon request
- I understand that failure to comply with any aspect of this agreement could lead to disciplinary action
- Upon the event that an iPad or laptop is lost or stolen, I will report the matter in writing to the School Business Manager & Subject Lead within 24hours. As per the disciplinary policy, any deliberate or malicious damage to school property could result in the deduction of wages for the equipment.

I agree to abide by this Acceptable Use Policy at all times

Date:



Signed (staff member/governor/volunteer/visitor):

Appendix 2: Information and Guidance for Parents and Carers



Information and Guidance for Parents and Carers

Shoreditch Park
Primary School

Online safety is concerned with safeguarding children in the digital world.

We encourage you to learn how to use new technologies and ICT (Information Communication Technology) in a positive way.

Online safety is not about restricting children, but educating them about the risks as well as the benefits so they can feel confident, safe and happy online.

To keep your children safer online:

- ✓ Think about how you guide your family in the real world and do the same in the digital world - don't be afraid to set boundaries and rules for your children
- ✓ Boundaries may be the amount of time children can spend on a computer, smartphone, tablet or games console, along with the types of websites they can visit or which apps you allow them to download (remember to ensure young children cannot download apps themselves, and must always seek your authorisation before using an internet-connected device)
- ✓ Encourage balanced use – switching off devices at mealtimes and before bedtime.
- ✓ Talk to your child. Share the experience of using technology with them - and ask them to show you how they use technology.
- ✓ Encourage your child to talk to you about anything they see or experience online which upsets or disturbs them.
- ✓ Talk to your friends, family and other parents about how they help their children to manage their digital world - you might pick up some interesting tips
- ✓ If your child reports a problem make sure you support them, report it or seek advice from family and friends you trust, or organisations such as Childline or the NSPCC.
- ✓ Discuss the importance of keeping personal details private. Personal data means full name, address, mobile phone number, email address and school name



o Remind children to be careful about uploading and sharing photographs. You must always ask permission before uploading or sharing a photograph of someone else or you may breach their right to privacy.

- ✓ Use a child friendly search engine, such as: www.kidrex.org.
- ✓ Agree the type of websites they can visit, and add those to your parental controls (on the computer or via your internet service provider).
- ✓ Agree which apps they can download to a smartphone or tablet. The minimum age for all social media sites is 13, so no primary school-age children should be accessing these services.
- ✓ Visit www.internetmatters.org/controls/interactive-guide/ for practical advice on how to activate parental controls for all types of devices around the home.
- ✓ Install antivirus software, filtering and firewalls for your home and mobile equipment.
- ✓ Remember that filters and firewalls are not always 100% effective and sometimes things can get past them – so we still have to think about our safety
- ✓ Locate the computer/laptop in a family room and don't allow webcams to be used unless with your consent and always in a family room under supervision.
- ✓ Save any abusive messages or inappropriate images for evidence purposes, and always report any such incident to an adult you trust, or organisations such as Childline, NSPCC or CEOP.
- ✓ Be aware of how to report nuisance calls, text messages, emails and other communication.



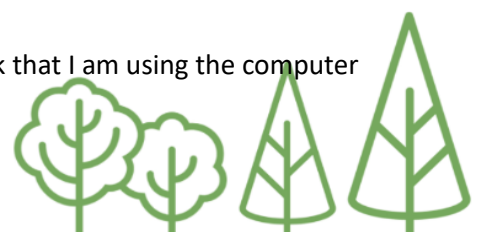
Appendix 3: Parent and child acceptable agreement

Parent and Child Acceptable Use agreement– 2023/2024

Child Agreement

As a child, I will respect these rules, with the support and guidance of my parents/carers, and staff at Shoreditch Park Primary. These rules will keep me safe and help me to be fair to others.

- I will only use the computers for purposes agreed by Shoreditch Park.
- I will only use the internet when a trusted adult supervises me.
- I will keep my logins and passwords secret.
- If I see anything that upsets me or I receive a message I do not like, I will not respond to it and I will show an adult I trust.
- I know I can always speak to an adult I trust if I see something on the internet that I don't understand or that upsets me.
- I will not attempt to visit internet sites that I know are banned.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless an adult I trust has given permission.
- I will only edit or delete my own files and not look at, or change, other peoples' files without their permission.
- I understand that my usage of the internet will be monitored and if I attempt to access websites I shouldn't be looking at, I will be asked about it.
- I understand the agreement for using computers, the internet, email and online tools safely and responsibly.
- I know the adults looking after me will help me to stay safe and check that I am using the computer to help me with my work.



Name:

Signature: Date:

Parent/Carer Agreement

- I have read and discussed the agreement with my child and confirm that he/ she has understood what the rules mean.
- I understand that the setting will use appropriate filtering and ensure appropriate supervision when using online and digital technologies.
- I understand that occasionally, inappropriate materials may inadvertently be accessed and accept that the setting will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet and other online tools outside of school, it is my responsibility to ensure safe and responsible use.

Name:

Signature: Date:





Appendix 5: online safety self-audit for staff

Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	



Online safety incident report log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6: online safety incident report log

