

ONLINE SAFETY POLICY



Chisenhale
Primary School

Confidence • Curiosity • Kindness

Date reviewed	October 2024
Reviewed by	Gemma Anidi
Approved by Governors	November 2025
Planned Review date	November 2026

1. Introduction.....	3
2. Roles and responsibilities	3
3. Teaching online safety.....	5
4. Filtering and monitoring.....	5
5. Security	7
6. Educating parents about online safety.....	7
7. Acceptable use agreement.....	7
8. Use of mobile and smart technology	7
9. Training and staff knowledge	8
10. Further information to support you	8

1. Introduction

Chisenhale Primary School is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to both educate and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

In line with Keeping Children Safe in Education, we aim to address the following four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

2. Roles and responsibilities

2.1 The governing body:

- Take overall responsibility for this policy and its implementation
- Read, and understand this policy
- Ensure the policy is reviewed and updated annually
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems

2.2. Headteacher:

- Ensure staff understand this policy
- Ensure the implementation of this policy is consistent across the school
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter

- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns

2.3 Designated Safeguarding Lead:

- Support the headteacher in implementing this policy
- Oversee the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead
- Work with Computing lead, IT technician and safeguarding team to address any online safety concerns or incidents, in line with our child protection and safeguarding policy
- Liaise with external safeguarding partners as necessary, including children's social care and the police and make referrals with the support of relevant colleagues and their expertise
- Ensure any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents
- Deliver staff training on online safety
- Provide regular updates regarding online safety incidents to the headteacher
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/safeguarding team and regular reports are received

2.4 IT technician

- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the school's ICT systems are secure and protected against viruses and malware
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/safeguarding team and regular reports are received

2.5 All staff and volunteers

- Read and understand this policy
- Assist with the consistent implementation of this policy
- Agree with and follow our acceptable use of IT agreement
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Refer any online safety safeguarding concerns to the DSL or a Deputy DSL by our standard reporting procedures, e.g. recording on CPOMs using appropriate categories.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.

2.6 Parents

- Understand the importance of children being safe online
- Read, understand and comply with this policy

- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access and who from the school (if anyone) will be interacting with their child
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online

3. Teaching online safety

In line with 'Teaching online safety in school,' published by the Department for Education in June 2019, we teach pupils about online safety and harms. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These skills are covered in Computing and PSHE lessons and during assemblies. As well as being revisited when pupils are using devices.

Throughout this, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online
- the risks posed by social media platforms
- how to recognise techniques used for persuasion
- unacceptable online behaviour
- how to identify online risks
- how and when to seek support
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online
- how elements of online activity can adversely affect a pupil's wellbeing

We recognise that there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We will ensure these pupils receive the information and support they need through ensuring that the curriculum has been reviewed to ensure all pupils can access it.

In addition, our school completes an annual risk assessment for online safety. We consider the updated non-statutory guidance (Jan 2023) from the [DfE on teaching online safety](#) and how we teach these elements.

4. Filtering and monitoring

Chisenhale Primary School uses LGFL as a filtering system. Our primary method of monitoring is through classroom organisation and supervision; however, we also use Impero software to support with monitoring. LGFL filtering covers our school network and any devices using the school internet/wifi. Impero monitors all chromebooks and laptops.

For details of what LGFL filters, please see this guide:

<https://d1xsi6mgo67kia.cloudfront.net/uploads/2020/01/LGfL-Appropriate-Filtering-Provider-Response-August-2023-LGfL.pdf>

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies, along with the IT technician, monitor the

effectiveness of this system through an annual check each September on testfiltering.com on a variety of devices. A record is kept of these tests.

The school takes care to not 'over block' content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

The DfE has published [filtering and monitoring standards](#) which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without reasonable impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

We at Chisenhale Primary School have done the following in relation to this:

DfE Filtering and monitoring requirements	Chisenhale actions
Identify and assign roles and responsibilities to manage filtering and monitoring systems	<ul style="list-style-type: none"> • The DSL/headteacher has overall responsibility for filtering and monitoring in school and dealing with any safeguarding concerns that arise. • The Senior leadership team makes sure staff understand their roles, reviews the effectiveness of our systems and oversees reports • IT service provider (Connetix) has technical responsibility for maintaining and managing our system • Teachers and support staff have the following responsibilities: <ul style="list-style-type: none"> ◦ Teach children about responsible digital behaviour, ethics, and the consequences of inappropriate online actions ◦ Notify if teaching about any topics which could create unusual activity on the filtering logs; or if think are any unreasonable restrictions affecting teaching/learning/admin tasks ◦ Report if witness or suspect unsuitable material has been accessed, or notice abbreviations or misspellings that allow access to restricted material
Review filtering and monitoring provision at least annually	<ul style="list-style-type: none"> • The DSL will oversee the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online. • The DSL and deputies, along with the IT technician, monitor the effectiveness of this system through an annual check each September on testfiltering.com on a variety of devices. A record is kept of these tests.
Block harmful and inappropriate content without reasonable impacting teaching and learning	<ul style="list-style-type: none"> • LGFL webscreen blocks harmful content, and is designed for education settings.

Have effective monitoring strategies in place that meet their safeguarding needs	<ul style="list-style-type: none"> Monitoring is included in all induction training for new staff as well as at least annually for all staff. Staff are reminded of the importance of monitoring and how Impero's software support this, but does not replace close supervision.
--	--

When the filtering and monitoring system detects concerning usage, we will record this on CPOMs and take appropriate action, including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact the DSL on safeguarding@chisenhale.towerhamlets.sch.uk

5. Security

Chisenhale Primary School has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies.

This includes safe search filtering with Google search and the Chrome browser, keyword and subject category blocking via Webscreen filtering and restricted internet connections through the London Grid for Learning (LGfL).

All internet-based activity on the school's systems is able to be retrospectively audited and traced for more information via the school's internet service provider, their security controls and its compliance with the government's KCSIE guidance.

See this article [KCSIE Response - LGfL](#) for more information in how the facility works and is implemented in schools across London.

6. Educating parents about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety, we have a subscription to 'National Online Safety' with an app, guides and videos available to all parents. Periodically we also offer parent workshops on online safety, as well as offering individual advice where appropriate or requested.

7. Acceptable use agreement

All pupils, parents, 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. Any breaches of this agreement can lead to steps taken in line with the school's code of conduct and staff disciplinary policy, and in where appropriate, the police and children's social care.

8. Use of mobile and smart technology

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children can sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To manage this and reduce risk, we do not allow children from nursery to Y5 to bring phones into school. Children in Y6 can bring phones when they are walking to and from school alone, but they must be handed into the office each

morning, where they will be locked in the safe until the end of the school day. Any phones found in school during the school day will be confiscated immediately.

Our Staff Code of Conduct outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

9. Training and staff knowledge

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. This will also include training on the filtering and monitoring system used by the school and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as relevant updates (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy 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 about online safety at regular intervals, and at least annually.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.
- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online, this can take the form of:
 - Online abuse, including sexual
 - Online harassment, including sexual
 - Cyberbullying
 - Misogynistic/ misandrist messages,
 - the non-consensual sharing of incident images, especially around chat groups,
 - and the sharing of abusive images and pornography to those who do not want to receive such content.
 - That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

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

10. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarded. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For **parents** the following websites could be of use:

- [Samaritans: Talking to your child about self-harm and suicide content online](#)

- [NSPCC Online Safety Guides for parents](#)
- Report harmful content at <https://reportharmfulcontent.com/>
- Report concerns to the NSPCC <https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/>
- [Thinkuknow](#)- how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed [here](#)

For **students** the following websites could be of use:

- [Mind](#)- mental health support
- [Togetherall](#)- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- [Samaritans' self-help app](#)
- [Kooth](#) is an online mental wellbeing community for young person
- Report harmful content at <https://reportharmfulcontent.com/child/>
- Report concerns to the NSPCC <https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/>

For **all staff and volunteers**, it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- [UK Safer Internet Safety](#)- teacher guides and resources
- <https://www.internetmatters.org/schools-esafety/>
- <https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools>

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy.
- Behaviour policy.
- Staff Code of Conduct inc. acceptable use of technology in the staff behaviour policy/ code of conduct.
- Anti-bullying procedures including cyberbullying
- [The Prevent Duty](#) and [The Prevent duty: an introduction for those with safeguarding responsibilities](#)
- [Meeting digital and technology in schools and colleges \(DfE\)](#)