Kensington Avenue Primary School

Online Safety Policy

Approved by: Governing	Local Governing Body	**Date:**	September 2024
Last reviewed on	September 2024		
Next review due by:	September 2025		
Version: 3			

Key People

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	**Gill Chamberlain**
Deputy Designated Safeguarding Lead / DSL Officers	**Justine Bristow (Deputy), Glenn Lillo (Officer) Pammy Bhambra (Officer)**
Link governor for Safeguarding	**Richard McIntosh**
Curriculum leads with relevance to online safeguarding and their role	**Henriette Schroder – PSHE** **Nadia Da Silveira – Computing Lead**
Network manager / other technical support	**Dean Dumont, Nadia Da Silveira**

Contents

1. Aims

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2024 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Child protection and safeguarding policy, Behaviour Policy or Anti-Bullying Policy)
- 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, portable 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
- 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 board

The governing board has overall responsibility for approving and monitoring this policy overseeing 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 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.

The governor who oversees online safety is Richard McIntosh

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on the acceptable use policy 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 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.

Responsibilities will also include;

Ensuring ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures.

Ensuring ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.

Ensuring the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles

Liaising with the designated safeguarding lead and ICT team on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

This list is not intended to be exhaustive.

3.3 The designated safeguarding lead

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

The DSL takes lead 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

- Ensuring “An effective whole school approach to online safety as per KCSIE
- Ensuring ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
- Updating and delivering staff training on online safety (Training will be deployed through Safesmart -Appendix 4 contains a self-audit for staff on online safety training needs)
- Working with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- 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 - Overall responsibility is held by the DSL
- Working with the ICT Team to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT team 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 (see appendix 6) 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
- 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

This list is not intended to be exhaustive.

3.4 The ICT Network manager & Computing Lead / ICT Manager

The ICT Network manager is responsible for:

- 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 – The school filtering and monitoring service provider is: LGFL School Protect / Home Protect
- Supporting the DSL to carry out an annual online safety audit as now recommended in KCSIE.
- Regular web filtering and monitoring checks consisting of scheduled reports conducted weekly with the ability to create on demand reports at any given instance.
- 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 monthly basis –Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 6) 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 and acceptable use policies

The Computing lead / ICT Manager is responsible for:

- Overseeing the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Working closely with the PSHE lead to embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives.”
- Underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing

This list is not intended to be exhaustive.

3.5 PSHE Lead

The PSHE is responsible for:

- Working closely with the Computing lead to embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives.”
- Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE
- Working closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

This list is not intended to be exhaustive

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers should sign and follow the relevant acceptable use policy in accordance with this policy, the school’s main child protection & safeguarding policy, the code of conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.
This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

All staff 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing the new DfE standards and relevant changes to filtering and monitoring – The DSL takes lead responsibility filtering & monitoring systems and processes in place
- Playing their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.
- Working with the DSL and ICT team to ensure that any online safety incidents are logged (see appendix 6) 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'

This list is not intended to be exhaustive.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Read and ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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
- Dedicated resources at: Parentsafe.lgfl.net

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 (appendix 4).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum carefully. Learning will be sequenced to establish understanding then build upon what pupils have already learned to identify subject content that is appropriate for their stage of development.

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

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.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE) ; Google Classroom. This policy will also be available on the school website and hard copies available from the school office.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use – LGFL School Protect / LGFL Home Protect
- Internet safety workshops / drop ins scheduled throughout the academic year.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

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. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) 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. 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 - Searching & confiscation

In line with DfE guidance , 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 identified in the school rules as a banned item for which a search can be carried out, 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 [the headteacher / DSL / appropriate staff member
- 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, in conjunction with the DSL / headteacher / other member of the senior leadership team] a suitable response should be decided. 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)

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, Gemini and Copilot.

Kensington Avenue 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.

Kensington Avenue Primary School will treat any use of AI to bully pupils in line with our Anti-bullying/Behaviour 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 / DPIA 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 (appendices 1 to 3). Visitors/contractors will be expected to read and agree to the school's terms on acceptable use where relevant (appendix 4).

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 appendices 1 to 4

8. Pupils using personal mobile devices (including wearable technology) in school

Pupils should not bring mobile phones or wear camera enabled smart watches to school. Pupils are only allowed to bring mobile phones in for agreed emergencies, travelling between school and home or where a known and recognised exception has been communicated to the school. During school hours (including after school clubs/events or activities organised by the school) phones must remain off and locked away by the pupil. Parents/carers are asked not to attempt to pupils on their mobile devices during the school day; urgent messages can be passed via the school office.

Also see the acceptable use policy (AUP) agreement which all parents/carers and pupils must adhere to (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device and/or the parent/carer being informed.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Maintaining up to date anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use policy, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice the ICT team

10. How the school will respond to issues of misuse and incidents

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on safeguarding and child protection, anti bullying, behaviour, data protection and internet acceptable use policies The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Any suspected online risk or infringement should be reported to ICT and the DSL on the same day using in place reporting tools. General concerns must be handled in the same way as any other safeguarding concern.

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 disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Where a visitor/contractor misuses the school's ICT systems or internet, or is in violation of the AUP agreement,this will be taken very seriously. We expect all visitors to respect our online safety policy and to help us keep our children safe.

The school will actively seek support from other agencies as needed (i.e. local authority, LGFL, NCA CEOP) and consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police. The school will inform parents/carers on online safety incidents involving their children.

11. 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 Safesmart training portal, emails and staff meetings and the online safety needs - self audit - Appendix 5).

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 DSL, Deputy and officers 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.

12. Monitoring arrangements

Reporting and logging of behaviour and safeguarding issues related to online safety will be collected by the DSL and ICT team. Regular checks are made to ensure filtering is active and appropriate blocking (including not over blocking) is in place. A manual incident report log can be found in appendix 6.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review will be supported by an annual online safety audit to identify new risks and challenges as this is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

Safeguarding & child protection policy	Acceptable use policies / Agreement
Code of conduct	Data protection policy and privacy notices
Behaviour policy	Complaints procedure
Anti Bullying Policy	

Appendix 1: Acceptable Use Policy (AUP) For pupils & parents/carers

Kensington Avenue Primary School

Acceptable Use Policy (AUP) For pupils and parents/carers

Date Approved	Sept 2024
Date to be Reviewed	Sept 2025
Version	7

Overview

At Kensington Avenue Primary School, we are committed to ensuring that all pupils use technology safely, respectfully, and responsibly. We ask all students to agree to and follow this Acceptable Use Policy, which outlines the rules for using the school's ICT systems, internet, and personal devices. By following these guidelines, you help us maintain a positive and secure online environment both at school and at home

When I use the school's ICT equipment, systems and internet **I will**:

- **Ask permission** from a teacher or adult before using the devices or internet.
- **Only use websites and programs** that a teacher or adult has said are safe and appropriate for me to use.
- **Tell my teacher** immediately if:
    - I select a website by mistake.
    - I see something that makes me upset or feel uncomfortable.
    - I receive messages from people I don't know.
- **Use the ICT equipment for educational purposes only.**
- **Be kind and respectful** to others, both online and offline.
- **Look after the school's ICT equipment**, and let a teacher know if something is broken.
- **Keep my username and password safe**, and never share it with others.
- **Never share personal information** (my name, address, telephone number) with people I meet online.
- **Respect copyright** by not copying work from the internet and always giving credit to the sources I use.
- **Visit safe websites** like www.thinkuknow.co.uk to learn more about online safety.
- **Report cyberbullying** immediately if I experience or see it.
- **Communicate politely** and respectfully online, remembering that posts can stay online forever.
- **Log off or shut down** the computer when I'm finished.

I will not:

- Access any **inappropriate websites** including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Try to bypass the **school's internet filter**, which is in place to protect me
- **I will not try to use social media** without permission and understand most platforms have a minimum age of 13I
- **Attempt to follow or befriend any members of staff on any social platforms.**
- **Open attachments or follow any links**, without first checking with a teacher (if not in Google classroom)
- **Use any inappropriate language when communicating online**, including in chatrooms / Google classroom
- **Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate**
- **Log in to a school device, Google classroom or other learning platform using someone else's details**
- **Arrange to meet anyone in person without first discussing it with my parent or carer, or without adult supervision**

I **understand** that the school will monitor the websites I visit, and that there will be consequences if I don't follow these rules.

I **understand** that all school devices are monitored, even if I use them at home.

Online Lessons and Google Classroom:

I will follow school rules when participating in virtual classrooms and always behave as I would in a physical classroom.

Mobile Phones and Wearable Technology:

I will not bring mobile phones or wearable smart technology (e.g., smartwatches) to school unless it's for exceptional circumstances, such as for emergencies or walking home alone.

Pupil Acknowledgment and Agreement (KS2):

I have read the rules for using the school's ICT systems, equipment, internet, and personal mobile devices, and I agree to follow them.

Print Name (pupil) …….....

Class……

Signed (pupil)……...

Date……..

Parent/Carer Acknowledgment and Agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out for using the school's ICT systems, internet, and personal devices, and I will make sure my child understands these rules.

Visit https://parentsafe.lgfl.net for helpful tips and resources to support online safety at home.

Print Name (parent/carer)…….....

Signed (parent/carer)……...

Date……..

Appendix 2: acceptable use agreement (staff, governors, volunteers)

Kensington Avenue Primary School

Staff/Governors/Volunteers Acceptable Use Policy (AUP)

Date Approved	Sept 2024
Date to be Reviewed by	Sept 2025
Version	7

Overview

At Kensington Avenue Primary School we are dedicated to providing a safe and nurturing environment for our pupils so ask all children, young people and adults involved in the life of Kensington Avenue Primary School to sign an Acceptable Use Policy, which outlines how we expect them to behave when they are on-site, outside of school, online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media.

The policy applies to all staff and governors whether employed directly by the school or via external contractor/agency. All staff and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policies. This AUP will help ensure the expectations regarding the welfare of pupils and safe and responsible use of technology is understood both for your behaviour as an adult and enforcing the rules for pupils.

This agreement does not provide an exhaustive list to our approach to online safety but is consistent with the school ethos, code of conduct, e-safety, safeguarding and UK GDPR policies & procedures, DFE child protection guidance, and the law.

This AUP is reviewed annually, and staff and volunteers are asked to sign it when starting at the school and/or whenever changes are made.

If you have any questions about this AUP or our approach to online safety, please speak to the Designated Safeguarding Lead (DSL) and/or ICT team.

The schools' DSL is Gill Chamberlain

The schools' ICT team are Dean Dumont and Nadia Da Silveira

The schools'/Trusts Data Protection Officer (DPO) is;
Data Compliance – The Education Space
3rd Floor. Boardman House. 64 Broadway, London E15 1NT
e:DPO@theeducationspace.co.uk
w:theeducationspace.co.uk
CR7 8BT

Data breaches are reported to:
Data Compliance – The Education Space
3rd Floor. Boardman House. 64 Broadway, London E15 1NT
e:DPO@theeducationspace.co.uk
w:theeducationspace.co.uk

(Breaches should be reported using the breach reporting form in the first instance but an email can be sent as a last resort alternative)

The Schools' internal UK GDPR contact is Dean Dumont

Policy scope

- I understand this policy should agree to read this policy in full, and by signing it confirm I have understood and will abide by all points below.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I am aware that this policy does not provide an exhaustive list so all staff should ensure acceptable use of technology is consistent and read in conjunction with other relevant school policies and procedures including but not limited to:

  - ➢ Child Protection and Safeguarding Policy
  - ➢ Online Safety Policy
  - ➢ Code of Conduct policy
  - ➢ Data Protection Policy
  - ➢ Data protection Impact Assessment (DPIA) procedure
  - ➢ Data Breach procedure
  - ➢ Subject Access Request (SAR) procedure

Use of Personal and Portable devices (Mobile phones/Smart Technology)

- I understand the following regulations apply to all electronic media, including but not limited to mobile / smart technology accessed on or from the School premises or used in a manner which identifies the individual user with the school (if on a school trip etc)

- I understand personal and portable devices such as mobile phones, smart watches, e-readers and any other form of smart technology equipped with a camera are allowed in school, but are not allowed to be used in classrooms (visible to pupils), pupil learning environments or sensitive areas, inclusive but limited to; cloak rooms, toilets, when children are changing, swimming) other than in exceptional circumstances, such as emergency situations

- I understand the use of personal devices used for taking images or recording personal information of individuals or school data is strictly prohibited and could lead to disciplinary action being taken

- I understand personal/portable devices (mobiles) should not be kept on your person as you walk around the school premises unless exceptional circumstances apply /in or travelling to the staff room or personal office.

Digital equipment, Systems and Technology

- I agree to use the school's digital technology, resources and systems for professional / educational purposes only and not bring my role into disrepute.
- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members
- I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.

- I will report any incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media to the DSL via the reporting system CPOMS
- I will not attempt to install, remove or repair any hardware without the approval of ICT.
- I acknowledge and accept that personally owned laptops, tablets or devices which can be connected to the internet and/or capture images must not be brought into school or used with learners without seeking prior permission from senior management or ICT. If the use of a device has been denied, it must not be brought back into school.
- I agree and accept that any computer, laptop, mobile phone or tablet loaned to me by Kensington Avenue Primary School is provided solely to support my professional responsibilities and must not be used for personal use or activity deemed inappropriate or excessive.
- Where I deliver or support remote learning with pupils I will only use learning platforms authorised or agreed by the school.
- During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.

Data protection, Cyber security and Web filtering

- As a trusted employee, I have a responsibility to protect the confidentiality and privacy of data in compliance with UK GDPR data protection principles. This is especially important for users with access to personal and special category data, pupil data, medical, health and social/emotional well-being records and financial information To prevent unauthorised access, sharing or disclosure I agree to ensure high levels of data-protection strategies and processes are adhered to at all times. This includes only accessing data you have authority or a legitimate business to do so, the use of strong passwords,the use of 2 Factor authentication, secure storage of files, folders and devices when not in use, not sharing or revealing user account information or allowing unauthorised individuals to access any systems or information within them.
- All employees with enhanced access and permissions to CPOMS must take all reasonable steps to ensure the confidentiality and security of the data it contains is protected in accordance with Safeguarding guidelines, UK GDPR and the Data protection policy of the School/Trust. Unauthorised access or disclosure of information may result in disciplinary action, up to and including dismissal.
- I agree to report any suspected breaches of confidentiality or privacy in accordance to UK GDPR compliance -. *See Data Breach Procedure.*
- If I have lost/misplaced (Temporarily or permanent) any school data, files, images, or property related to the school that could compromise the identity of any individual (including myself, I will report this to ICT and the external DPO using the report a breach form - (see reporting a Data breach procedure)
- I will seek guidance if unsure about sharing, accepting (including hyperlinks and attachments in emails) or exchanging data with a person, system or service before doing so.
- I understand I am not authorised to sign up or register pupils or the school to 3rd party platforms without following procedures and gaining approval from SLT and ICT first. *See DPIA procedure*. A DPIA checklist must be carried out first before any subscriptions or sharing of data can be agreed.
- I agree to maintain good practice and acceptable standards in regards to secure file storage and deletion practices on all systems data is stored in accordance with UK GDPR and the schools network and confidentiality protocols. Files must be kept up to date and not stored for keepsakes / excessive periods of time without a supporting legal basis evidenced.
- I will not compromise the security of the school network or systems used to process, store or access data by leaving a device/screen unlocked or unattended. Devices must be password/passcode locked when left unattended and logged off after use / locked away at the end of the day.

- I will ensure all documents, data, photos, records, information etc. are saved, accessed and deleted in accordance with UK GDPR and the schools retention, network and confidentiality protocols and procedures.
- Any images or video of pupils must always be appropriate and should only be taken with school equipment. I understand images can only be taken and published if the school have parental consent to do so.
- I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2024, now led by the DSL
- I will not attempt to bypass or remove any filtering or security put in place on any KAPS owned device or system.
- I will prepare and check all online sources and classroom resources before using for accuracy, copyright and appropriateness (including the use and support of AI tools/chat bots).
- I will flag any concerns about overblocking or access restrictions to the DSL.
- When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe
- I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I might identify.
- I will not attempt to access or remove data / financial information from any of the KAPS owned devices or systems used unless authorised to do so.
- I will not save files locally (to the computer's C: drive). Files must only be saved to approved and accessible locations on the network or cloud drives owned/maintained by KAPS and where ICT have access.
- I agree not to send sensitive information by email unless it is encrypted/password protected – Kensington Avenue Primary School currently uses the following tools: Egress, 7-Zip and USO-FX.
- I agree that the use of non-encrypted memory sticks is not permitted in school and not for use to transfer, store or carry confidential, sensitive or person identifiable data. It must be recognised that this data comes under the UK GDPR and is subject to the school's Data Protection Policy – ICT can encrypt any USB memory stick that isn't originally encrypted when purchased.
- I will ensure if permitted, any confidential data, copied, transferred or stored on a portable device is protected by encryption and that I follow KAPS data security protocols.
- If working from home, I understand devices used and any information (physical or digital) related to the school must be kept secure and not shared with members of the household or nearby community.
- I understand the data protection policy requires that any information seen by me with regard to service users, held within the KAPS and LA's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I agree to add the mandatory email disclaimer to my email signature (provided by ICT) as a means to support any accidental sending of emails to an incorrect/unintended recipient.
- In order to keep data safe and avoid viruses and cyber attacks, I will take care when reading emails with links, attachments or messages. All emails should be treated as suspicious at first glance. Any requests for information or instructions regarding resetting of passwords may be Phishing attempts. If unsure, do not click on links or open email attachments as they could contain Malware or be Spam. Alert ICT immediately if you are concerned or suspicious about an email or sender.
- I must report any accidental access to, or receipt of inappropriate materials, or web filtering breach to the DSL and/or ICT team immediately.

- If I suspect a device or system has been damaged or affected by a virus or other malware, I will report this to ICT as soon as possible/on discovery.

Conduct and communication in school, online or via telephone

- I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language
- I will only use the currently approved email system in place for communications related to work at Kensington Avenue Primary School. This is currently: LGFL staff mail
- I will only use approved systems to communicate with pupils/parents/carers or to send notices or announcements on behalf of the school. In this organisation the systems used are: Internal work phones, LGFL staff mail, Arbor, Parentmail, the school website, Google Classroom/Workspace, and Twitter.
- I will ensure any communication with parents or pupils via email, learning platforms, message systems or other electronic means remain professional at all times and agree not to give out any of my own personal contact details such as email or phone numbers.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not browse, download or send material that could be considered offensive or of an extremist nature to anyone.
- I will not support or promote extremist organisations, messages or individuals
- I will not publish or distribute work that is protected by copyright.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff.
- I will not download or store images of pupils or staff at home on personal devices.

Use of Social Media

I agree to ensure that my online status and reputation is compatible with my professional role and in accordance with the schools code of conduct policy.

- I will take appropriate steps to protect myself and will ensure that any social media platform or profile I own, create or contribute to are not confused with my professional role.
- I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role and will ensure I have adequate privacy/security settings activated.
- I understand that personal online communication tools or platforms (Instagram, Facebook, Tik Tok, LinkedIn, Youtube, Twitter etc) must not be used with children's families and I will not communicate or 'befriend' any children and/or families using such methods.
- If approached or contacted by a pupil or parent online, I will not respond and should report it to the school Designated Safeguard Lead (DSL) if I have any questions or concerns regarding safeguarding and professional practice online.
- I will not share my personal contact information with pupils.
- I will not add or accept friend requests, or engage in communications with pupils on personal social media platforms. Pupils are not not allowed to make friend requests and are discouraged from 'following' staff, governors, volunteers or contractors.
- I will not upload any material or images associated with the school or trust without consent or permission being sought.

- I understand that permission/consent must be sought before uploading photographs, videos or an other information about other people
- I will not download or access or distribute any materials which are illegal, inappropriate or likely to cause harm, offence harassment or needless anxiety to another person..
- I will not engage in any online activity or behaviour that could compromise my professional responsibility or bring the school or trusts name and reputation into disrepute.
- I will not discuss or share information or personal data relating to pupils, staff, or parents/carers of the school or trust on any social media platform.
- I will alert the Headteacher if I feel the online behaviour of a member of staff may be a cause for concern or inappropriate.

Remote Access / Working from home

- I agree and accept that if I access school used systems or resources remotely (such as from home), I must use approved methods and tools to gain access, and follow e-security protocols. Current methods are myUSO, LGFL Freedom to Roam, and 2 Factor Authentication.
- I agree to keep my working environment and background free from sensitive information if on camera or recording material to broadcast at a later date(where possible use software filters to blur out backgrounds of family photos and backgrounds).
- I agree to sign a loan agreement form before taking any school ICT equipment home and accept the terms and conditions as per the schools Acceptable Use Policy.
- I will make sure that if any equipment and/or accessories (e.g. laptops, iPads, staff tags, camera leads/chargers) are misplaced, lost or stolen **I will report it within 24hrs**; I will also refer to the reporting a data breach procedure for guidance if applicable.
- I accept that equipment loaned to me is my responsibility and there may be costs at my own expense applicable to repair or replace any equipment and/or accessories lost or stolen whilst in my possession due to exposure to a non-insured risk and/or failure to undertake proper care.
- If I use my own equipment to access the networks or online systems from home, I will ensure my device has a separate user profile and has an up to date anti virus and malware protection program installed. If you are unsure how to check, please speak to ICT before attempting to use personal devices for remote access.
- To safeguard the integrity and security of the school network,I will not attempt to connect to the school network using a public wifi hotspot provider such as free public access points in cafes.
- I will ensure that school equipment loaned to me is always stored in a safe place and locked away at home away from unauthorised access when not in use.
- I understand I can be held accountable for unauthorised and/or inappropriate use of the school network or systems leading to disciplinary procedures being invoked.
- I agree to conduct myself professionally online at all times and to avoid any behaviour which could bring the school name and reputation into disrepute.

I have read, understood and agree to comply with this policy inclusive of all points listed above. I understand that failure to comply with the terms of this policy may result in disciplinary proceedings. [Acceptance and read receipts digitally via Safesmart will act as your signature]

Acknowledgment and Agreement

Print Name …….....

Role……

Signature…….

Date……..

Appendix 3: Acceptable use agreement (Visitors, Contractors)

Kensington Avenue Primary School

Visitor & Contractor Acceptable Use Policy (AUP)

Date Approved	Sept 2024
Date to be Reviewed	Sept 2025
Version	7

Overview

At Kensington Avenue Primary School we are dedicated to providing a safe and nurturing environment for our pupils so ask all children, young people and adults involved in the life of Kensington Avenue Primary School to sign an Acceptable Use Policy, which outlines how we expect them to behave when they are on-site, online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media.

Visitors and contractors are asked to sign this document to ensure they are aware and understand the schools expectations regarding safeguarding, online safety and responsible use of technology during their visit which applies to, but is not exclusive to laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies

This agreement does not provide an exhaustive list to our approach to online safety but is consistent with the school ethos, code of conduct, e-safety, safeguarding and GDPR policies & procedures, DFE child protection guidance, and the law.

If you have any questions during your visit, you must ask the person accompanying you and/or or the Designated Safeguarding Lead (DSL), or the IT team (where appropriate)

If questions arise after your visit, please notify the school office.

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. I will never attempt to arrange any meeting with a pupil, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
3. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
4. If I am given access to school-owned devices, networks/Wi-Fi access, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - I will not attempt to access any pupil / staff / general or sensitive school data unless expressly instructed/allowed to do so as part of my role
    - I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
    - I will protect my/any issued username/password and notify the school of any concerns
    - I will abide by the terms of the school Online safety and Data Protection Policy protections
    - I understand that my online activity will be subject to the school's filtering and monitoring systems, and that any attempts to access content which is illegal or inappropriate for a school setting, may result in further action as per the safeguarding procedures and may result in termination of contract.

5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
6. I will not engage in deabtes or reveal any information on social media or in private about the school or trusts that could bring name or reputation into disrepute and/or show the school in a bad light or could be perceived to do so.
7. I will not do or say anything to undermine the positive online safety messages that the school disseminates to pupils and will not give any advice on online safety issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – If this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).
8. I understand that children can be abused and harmed when using devices and I will report any behaviour (no matter how small) which I believe may be inappropriate or concerning in any way to the **Designated Safeguarding Lead - Gill Chamberlain** (if by a child) or **Headteacher – Clare Cranham** (if by an adult).
9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.
10. I will behave in a professional and responsible manner at all times and understand that failure to do so may result in further action being taken and could result in the termination of my contract.

To be completed by the visitor/contractor:

I have read, understood and agree to comply with this policy inclusive of all points listed above. I understand that failure to comply with the terms of this policy may result in disciplinary proceedings including termination of agreements / contracts.

[If received digitally via Safesmart smartlog, Acceptance and read receipts will act as your signature]

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date / time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name / role / date / time: _____

Appendix 4:

This appendix outlines the Guest Wi-Fi Acceptable Use Policy (AUP) for visitors accessing and using the schools Guest network.

KAPS ‘Guest WiFi’ Access – Acceptable Use Policy (AUP) 2024-25

THE USE OF OUR GUEST Wi-Fi - ‘KAPsNet Guests ONLY’

Kensington avenue primary school is able to provide guests and visitors (upon request from the main office/the person you are here to visit) conditional access to our Guest ‘Wi-Fi’ network during your visit according to this Guest WiFi Wireless Networking Acceptable Use Policy (the “Policy”) as a free, non-public service for the duration of their official visits.

Access is monitored and filtered to comply with our statutory safeguarding, e-safety and GDPR obligations. The IT infrastructure through which you connect is owned by the school, and may only be used by guests to access the Internet and e-mail to research information and to communicate with other users during their visit here.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and e-mail sent or received if they are found to contravene any of our policies or are inappropriate or illegal.

Visitors are expected to make responsible and appropriate use of the school’s Wi-Fi network during their stay. It is expected that visitors will comply with strict standards set out below.

Guidelines

These are guidelines to follow to protect personal privacy, acceptable use, fair usage and the integrity of the network.

1. All Internet activity should be appropriate to professional activity or education.
2. Use for personal financial gain, political purposes or advertising is not permitted.
3. Posting anonymous messages, accessing any chat rooms and forwarding chain letters is not permitted.
4. Do not interfere with the operation of the network by attempting to install or distribute illegal software, shareware, or freeware or other data files.
5. Do not violate copyright laws.
6. Do not view, send, or display offensive messages or pictures.
7. Do not share or disclose the password you have been allocated with another person.
8. Do not abuse network capacity and be mindful of the uses you are making of this service.

9. Remember the service is filtered and not all of your apps or the websites you visit or other on-line services which you make use of will work as they do from your normal network connection.
10. Our Guest network is provided "as is" without warranties of any kind, either expressed or implied. Connecting is at your own risk.
11. We have other restrictions in place regarding the use of cameras on Smartphones, Tablets and other IT Devices – those rules take precedence – nothing here permits the use of cameras where another policy would deny it.
12. Do not attempt to access any folders or files on our network unless they are being loaded from our public website.
13. Your access to the network may be blocked, suspended, or terminated at any time for any reason
14. Be Prepared to be held accountable for your actions if the Rules of Appropriate Use are violated.

Summary

Use of the Kensington Avenue Primary School Guest Wi-Fi network requires you to log-on to the network with the assigned voucher code or password. By logging on, you agree to abide by this and other policies that apply during your visit. You are to keep the password information secure and not share it with anyone. You accept that logs of any activity may be maintained in line with our retention policy and that in the event of any inappropriate use may be accessed and produced in evidence of any investigation. Serious misuse may result in prosecution.

Full Name…….....(Printed) Date.....

Signature.....

Job title.....

Reason for visit……

Length of visit - From:……/……/…… To:……/……/……..

OFFICE USE ONLY

Voucher ID Number: (Valid for 1 day unless specified)_____

Guest Wifi password provided: Y……N…..

Appendix 5: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
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?	

Please hand in or email to:

Designated Safeguarding Lead (DSL) - Gill Chamberlain - Gchamberlain@kaps.croydon.sch.uk

ICT team - Itsupport@kaps.croydon.sch.uk

Appendix 6: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**