EDWARD PAULING
Primary School
learning to succeed together

E-Safety and Online Policy

Policy Status	Final Policy
Responsibility for this policy lies with (Headteacher, Full Governing Body, Community and Premises, Curriculum or Finance & Staffing Committee)	Full Governing Body
Date written/last review	February 2026
Ratified by Governing Body	March 2026
Date of next review	February 2027

Contents

Our Vision for E-Safety and Online usage

At Edward Pauling Primary School, we acknowledge the integral part that the internet plays in life for education, business and social interaction. The safety and wellbeing of our children is paramount when our adults and children are using the internet. We aim to provide the school community, including all staff, governors, volunteers, children and parents, with our overarching principles that guide our approach to online safety and ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. This policy should be read in conjunction with the following policies (Appendix 1) and also takes into account regular updates and changes in legislation and government initiatives (Appendix 2).

Our Aims for E-Safety and Online usage

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 (which we refer to as 'mobile phones')
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Teaching and Learning

At Edward Pauling Primary School, all children are taught to use the internet appropriately, safely and effectively, and are educated in the effective use of the internet in research including the skills of knowledge, location, retrieval and evaluation. Our children are taught how to evaluate Internet content and to comply with the laws of copyright, are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

Our curriculum has been adjusted to consider when children are introduced to email skills, which are taught within the school filtering system, and when children use digital devices for taking photographs or create short films.

Our children are taught to use technology safely and respectfully, keeping personal information private, and to be able to identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies. We use published schemes of work to implement our computing curriculum and to support the consistent teaching of online safety in an age appropriate manner; currently we use *Purple Mash* (Computing Curriculum), guided by the PSHE Association to implement our PSHE Curriculum and are guided by *Development Matters* and *Think Equal* to support teachers in EYFS.

By the **end of primary school**, our children 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

To further raise the profile of Online Safety and in response to online safety concerns we plan and deliver content via: weekly safe and sound assemblies, age appropriate homework, discreet lessons, class visits from The Metropolitan Police Service (MPS) dedicated schools team, previously known as Safer Schools Officers (SSOs), Safer Internet themed days, parental workshops and Anti-Bullying theme days.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place so children are not able to access harmful or inappropriate material but at the same time leaders are careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At Edward Pauling Primary School, the internet connection is provided by London Grid for Learning (LGfL), this means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called School Protect, which is made specifically to protect children in schools. Strict procedures are in place to ensure our children, staff and wider community's data are kept on line and passwords are secure. Furthermore, users usage in school is monitored by a programme called SENSO, and DSLs are responsible for monitoring.

Handling online safety incidents and concerns

At Edward Pauling Primary School, we take all reasonable precautions to ensure online safety, but recognise that incidents will occur both inside and outside school. We recognise that incidents that occur outside school will continue to impact our children when they come into school or during extended periods away from school.
All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's Child Protection and Safeguarding Policy. Any suspected online risk or infringement should be reported to a Designated Safeguarding Lead (DSL) on the same day, ideally by the end of the lesson.

Any concern or allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents or carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law, particular procedures are in place for cyber-bullying, sexting and upskirting (Appendix 2).

In the event of an incident, we will evaluate whether reporting procedures are adequate for any future closures, lockdowns, periods of isolation etc. and make alternative provisions in advance where these might be needed.

Roles and Responsibilities

The governing board

The governing board 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's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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 Ms Sarah Scott, Safeguarding Governor and Ms Lesley Connor, Deputy Child Protection Governor.

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

The Headteacher

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

Designated safeguarding leads (DSLs)

Details of the school's designated safeguarding leads (DSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSLs take 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

- 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with external ICT school support (provided by Platinum ICT) to make sure the appropriate systems and processes are in place
- Working with the headteacher, external ICT school support 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (on CPOMS) 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 (appendix 2 contains a self-audit for staff on online safety training needs)
- 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.

External School Support

Our external school support 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
- 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 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

This list is not intended to be exhaustive.

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
- Be aware of Hounslow Early Help offer- https://www.hounslow.gov.uk/downloads/file/10055/targeted-early-help-leaflet-for-professionals

  To make a referral please use the Children's Social Care Referral Portal- https://earlyhelp.hounslow.gov.uk/web/portal/pages/professional

- Should exercise professional curiosity and know what to look for so they can identify cases of children who may need help or protection.

- Respond 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'**
- 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 (appendix 3).
- Knowing who is responsible for the filtering and monitoring systems and processes, and being aware to report all incidents to a DSL.
- Working with the DSL to ensure that any online safety incidents are logged (on CPOMS) 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

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 3)
- 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 (appendix 3).

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
Online safety topics for parents/carers – Childnet
Parent resource sheet – Childnet

Cyber Bullying

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 Behaviour and Anti-Bullying policy.)

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 shares information/leaflets on cyber-bullying to parents/carers using our social media platforms or parent mail 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 and Anti-Bullying 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.

A 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.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Refer to Mobile Phones in School Policy for further guidance.

Any use of mobile devices in school by pupils must be in line with our use of mobile phones in school policy, which is in line with DfE guidance https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools

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.

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 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 or DSL.
- 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 staff member in conjunction with the DSL or Headteacher 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 (or equivalent) 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.

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 and Google Gemini.

Edward Pauling 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Edward Pauling Primary School will treat any use of AI to bully pupils very seriously, in line with our Child Protection and Safeguarding Policy and our Relationship 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/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff. Any use of Artificial Intelligence should be carried out in accordance with our Safeguarding policy.

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 can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- 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
- Installing 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
- Work devices must be used solely for work activities
- If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on: Behaviour and Anti- Bullying, Behaviour and ICT acceptable use. 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 disciplinary procedures and 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.

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 (Prevent training).

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, e-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:
    1. Abusive, threatening, harassing and misogynistic messages
    2. Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    3. Sharing of abusive images and pornography, to those who don't want to receive such content
    4. 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.

All **pupils** will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Monitoring Arrangements

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

This policy will be reviewed every year by the Computing Lead and School Senior Leadership. 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.

Appendix

Appendix 1- Relevant policies and Statutory guidance to be read in conjunction

Keeping Children Safe in Education https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
Teaching online safety in schools https://www.gov.uk/government/publications/teaching-online-safety-in-schools
Searching, screening and confiscation in schools https://www.gov.uk/government/publications/searching-screening-and-confiscation
Mobile Phones in School Policy https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools
Child Protection and Safeguarding Policy
Whistleblowing Policy
Data Protection Policy
Relationship Policy
RSE Policy
PSHE Policy
Computing Policy

Appendix 2- 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?	

EDWARD PAULING Primary School
learning to succeed together

Acceptable Use Policy

EYFS and Key Stage One

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day (childrenscommissioner.gov.uk/our-work/digital/5-a-day/) and:	✓
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

Signed

EDWARD PAULING
Primary School
learning to succeed together

Acceptable Use Policy

Key Stage Two

My name is _____

1. I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I am using them at home.
2. I do not behave differently when I'm learning at home, so I don't say or do things I would not do in the classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. I do not just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. I will not share or say anything that I know would upset another person or they would not want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. I keep my passwords to myself and reset them if anyone finds them out. Friends do not share passwords!
7. I do not click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. I will not get into trouble, but I must not share it. Instead, I will tell a trusted adult. If I make a mistake, I do not try to hide it but ask for help.
10. I communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
11. I am careful when someone wants to be my friend. Unless I have met them face to face, I cannot be sure who they are.
12. I check with a parent or carer before I meet an online friend the first time; I never go alone.
13. I do not stream live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

14. I keep my body to myself online – I never get changed or show what is under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. I say no online if I need to – I do not have to do something just because someone dares or challenges me to do it, or to keep a secret. If I am asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. I tell my parents or carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I am doing.
17. I follow age rules – 13+ games and apps are not good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
18. I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
19. I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
20. I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
21. I am part of a community – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
22. I respect people's work – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
23. I am a researcher online – I use safe search tools approved by my trusted adults. I know I cannot believe everything I see online, know which sites to trust, and know how to double check information I find. If I am unsure I ask a trusted adult.

I have read and understood this agreement.

My trusted adults are:

_____ at school

_____ at home

Signed

Date: / /

EDWARD PAULING Primary School
learning to succeed together

Acceptable Use Policy

Parent

1. I understand that Edward Pauling Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images or videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images or video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, they will need positive input from school and home. I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screen time and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc…
8. I understand that my child needs a safe and appropriate place to undertake remote learning if school is closed (similar to regular online homework). When on a video call with school, my child will be in an open environment where an adult can support if needed (not alone in their bedroom). My child will be fully dressed and not in bed, and the camera angle will point away from any personal information or private spaces. Where it is possible to blur or change the background, I will help my child to do so.

9. If my child has online tuition for catch up or in general, I will refer to the Online Tutors – Keeping children Safe (https://static.lgfl.net/LgflNet/downloads/online-safety/posters/LGfL-DigiSafe-Online-Tutors-Safeguarding-Guidance.pdf) poster and undertake all necessary checks where I have arranged this privately, ensuring they are registered, safe and reliable. I will ensure any on-line tuition sessions will be undertaken in the room where I'm present and ensure that my child knows that tutors should not arrange new sessions or online chats directly with them.
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
12. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which they have signed, and a copy is available on request from the school office. I understand that my child will be subject to sanctions if they do not abide by these rules.
13. I can find out more about online safety at Edward Pauling Primary School by reading the full Online Safety Policy, that is published on our school website (https://www.springgroveprimary.london/about-us-2/8420-2/) or a copy can be requested from the school office. If I have any concerns about your child's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school please speak to the Headteacher or your child's class teacher.

~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

_____

Name/s of parent / guardian: _____

_____

Parent / guardian of: _____

Date: _____
~~~~~~~~~~~~~~~~~~~~~

ONLINE TUTORS
KEEPING CHILDREN SAFE

GUIDANCE FOR PARENTS & CARERS

YOU MIGHT GET A TUTOR FROM SCHOOL, THE NATIONAL TUTORING PROGRAMME, A GOOGLE SEARCH OR A RECOMMENDATION. BUT ANYONE CAN CALL THEMSELVES A TUTOR, SO HOW CAN YOU KEEP YOUR CHILDREN SAFE WHILE THEY CATCH UP?

1) Select the right tutor

- Get to know them first - ask about qualifications, experience (freelance? umbrella body?) & approach
- Take up references and speak to them if you can
- Ask to see a DBS (criminal record) check. NB - private tutors can only get the basic check; (don't let a DBS give you a false sense of security though)
- Find out which platform they will use and its safety features

2) Establish clear rules

- Sessions must always be arranged via you; the tutor should not contact your child directly between sessions, send private messages or change communication platform
- A tutor is not a friend – they should behave in a professional way, like a teacher
- Sessions must not be recorded without your approval
- Try to be in the room for all sessions, especially for younger children, and certainly the first time
- Your child should not join a session from a bedroom. If this is unavoidable, pop in frequently, ensure they are fully dressed at all times, point the camera away from beds & personal information, and blur or change the background

3) Make sure your child knows

- The rules apply to them and the tutor
- A tutor is a teacher not a friend
- Neither tutor nor child should share personal information, private messages or photos & videos
- They must never meet without your approval or communicate on a different platform
- Who their trusted adults are at home and school
- They can tell you if they are asked to keep a secret or anything happens or is said that is strange or makes them feel uncomfortable, scared or upset

FIND MORE SAFEGUARDING RESOURCES TO SUPPORT PARENTS AT PARENTSAFE.LGFL.NET LGfL DigiSafe

Appendix 5 – Online Safety Incident Report Log

EDWARD PAULING Primary School
learning to succeed together

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**