Old Park Primary School & Nursery

Online Safety

Reviewed: **October 2026**
Next Planned Review: **October 2027**
Person responsible: **J Foster**

Aims:

Our school aims to:

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

Online Safety and Safeguarding:

The school recognises that online safety is an integral part of safeguarding and child protection. Online risks can occur both inside and outside school and may overlap with other safeguarding concerns, including child-on-child abuse, sexual harassment, child criminal exploitation, child sexual exploitation, radicalisation, mental health concerns and attendance issues. All concerns will be managed in accordance with the school's Child Protection and Safeguarding Policy.

The key categories of risk are:

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, extremism, and manipulated, AI-generated or deepfake content designed to mislead, exploit or harm individuals.
- **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.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Generative artificial intelligence (AI) tools, such as Microsoft Copilot, ChatGPT and Google Gemini, are becoming increasingly accessible to children and adults. The school recognises both the educational opportunities and safeguarding risks posed by AI technologies, including misinformation, inappropriate content, privacy concerns and academic integrity. Staff will assess risks before introducing AI tools and ensure any use complies with safeguarding, data protection and educational requirements.

Legislation and guidance:

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

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

It also refers to the DfE's guidance on protecting children from radicalisation.

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

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 Safeguarding and Online Safety Governor will undertake appropriate safeguarding and online safety training to support effective oversight of the school's online safety arrangements.

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 Governing Body will receive an annual report on the effectiveness of filtering and monitoring systems, including any safeguarding themes, trends or incidents identified.

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 Link Governor for Safeguarding and Online Safety is **Sally Lill.** The Link Governor provides strategic oversight and assurance regarding the school's online safety arrangements.

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 (Appendix 3).
- 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.

The designated safeguarding lead:

Details of the school's designated safeguarding leads (DSL's) are set out in our safeguarding policy. The DSL and Deputy DSLs take lead responsibility for online safety within the school.

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with Telford and Wrekin and the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are recorded on CPOMS and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or Governing Board .
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

The ICT manager:

The ICT manager is responsible for:

- Working with the school's ICT support provider, Telford & Wrekin ICT Services, and the ICT Manager to ensure appropriate systems and processes are in place.
- 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.
- Operational responsibility for filtering and monitoring with the Headteacher and Lead DSL, who will review systems regularly and ensure concerns are acted upon promptly.
- Ensuring a review of our filtering and monitoring systems annually.
- 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 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.

All staff and volunteers:

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the headteacher and school ICT manager.
- Following the correct procedures by liaising with the headteacher and ICT manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged 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.
- 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'.

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.

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

The school recognises the important role that parents and carers play in helping children stay safe online. Parents and carers are encouraged to engage with their child's online activities, discuss safe and responsible use of technology and make use of the following sources of information and support:

- National College (National Online Safety): www.nationalcollege.com/guides
- NSPCC Online Safety Hub: www.nspcc.org.uk/keeping-children-safe/online-safety
- Internet Matters: www.internetmatters.org
- Childnet: www.childnet.com
- UK Safer Internet Centre: www.saferinternet.org.uk
- CEOP Safety Centre: www.ceop.police.uk

The school will also provide parents and carers with updates, guidance and information about emerging online safety risks where appropriate.

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 3).

Educating pupils about online safety

Pupils will be taught about online safety as set out by the National Curriculum computing programmes of study. The school will also ensure it meets the requirements set out within the guidance on relationships education, relationships and sex education (RSE) and health education.

Pupils will learn how to evaluate information online critically and recognise misinformation, disinformation and manipulated digital content. Information regarding our safeguarding curriculum and friendships relationships curriculum can be found on our school website: https://www.oldparkprimary.co.uk/page/?title=Subjects&pid=41

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:

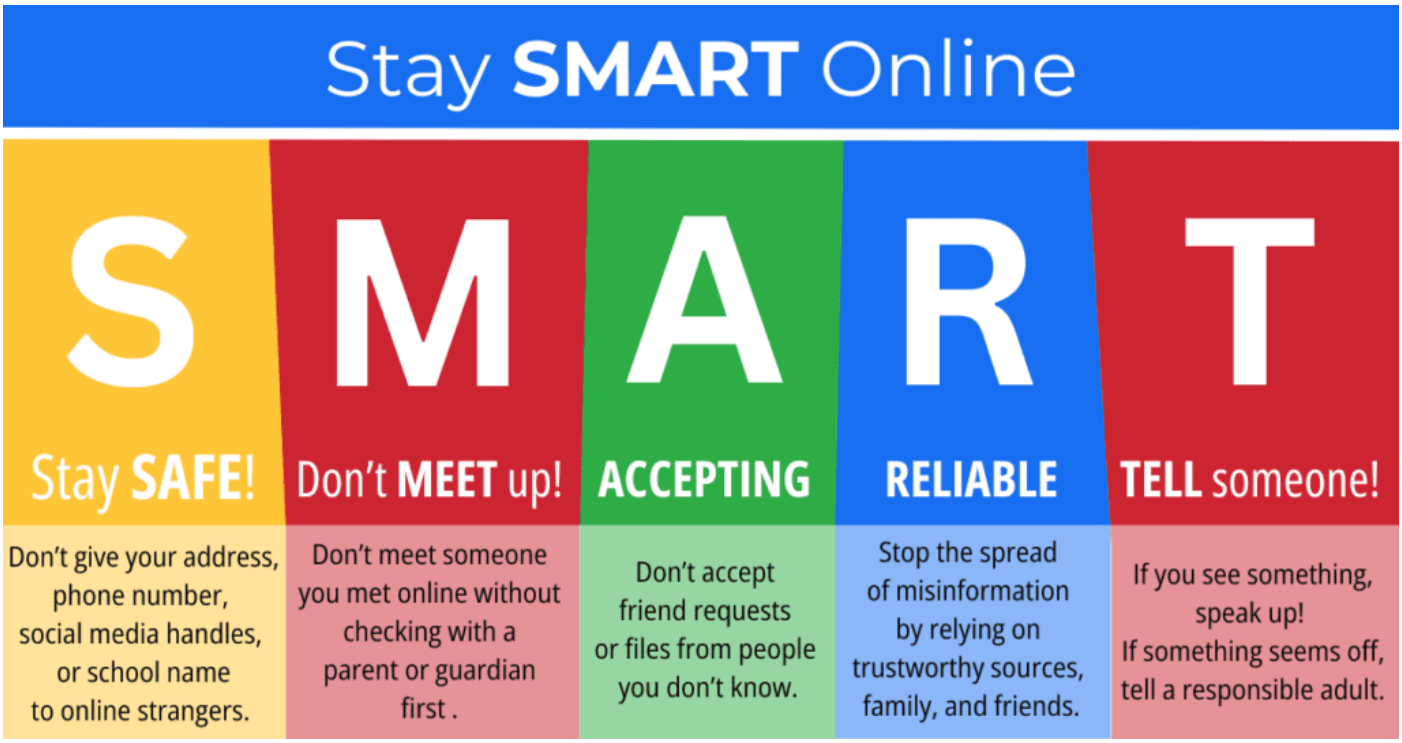
- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

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.



Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety through:

- This policy will be shared with parents/carers.
- Letters or other communications home.
- Sharing of school specific, local and national online safety concerns when needed.
- Social media posts such as WakeUpWednesday. The National College | #WakeUpWednesday
- Informing them of the filtering and monitoring systems that are used in school and how they work.
- Face to face and online workshops for parents focused on online safety.
- Sharing on local intelligence from the police if necessary.

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.

Cyber-bullying

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 the school's Child-on-Child abuse policy.)

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying, 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 within our friendships and relationships curriculum, and other subjects where appropriate.

All staff, governors and volunteers 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 child-on-child 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.

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:

- Assess 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.
- 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 headteacher/other member of the senior leadership team/DSLs 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 a 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 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) and emerging technologies

Generative artificial intelligence (AI) tools, such as Microsoft Copilot, ChatGPT and Google Gemini, are becoming increasingly accessible to children and adults. The school recognises both the educational opportunities and safeguarding risks posed by AI technologies, including misinformation, inappropriate content, privacy concerns and academic integrity. Staff will assess risks before introducing AI tools and ensure any use complies with safeguarding, data protection and educational requirements.

Emerging technologies are examined by the Telford and Wrekin IDT support team for educational benefit and a risk assessment will be carried out before use in school is allowed.

Acceptable use of the internet in school

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

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

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

Pupils using mobile devices in school

The DfE's mobile phone guidance says that the use of mobile phones should be prohibited throughout the school day.

- Pupils must not use their mobile phones during the school day, including during lessons, in the time between lessons, at breaktimes and at lunchtimes, unless explicitly authorised by a member of staff (for example, for a specific medical reason).
- Only pupils in Year 5 and 6 are permitted to bring a mobile phone to school.
- Requests for exceptions in other year groups will only be considered in exceptional circumstances and must be agreed by the headteacher.
- Upon arriving at school all phones must be turned off and given to the class teacher.
- The school will maintain a secure process for the collection and return of mobile phones.
- Mobile phones are stored within a locked box for the entirety of the school day and are given back to pupils at the end of the school day.
- Pupils with certain medical conditions may be permitted to have their phone on them in school – this will be part of the care plan and agreed with professionals.

Smart devices capable of photography, video recording, messaging or internet access will be treated in the same way as mobile phones unless specifically authorised by the school. Further information on the use of mobile phones can be found in our mobile phone policy 2026.

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.
- 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.
- 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 school ICT manager.

Social networking

The school appreciates that many staff will use social networking and tools. The use of social media networking tools and how to relates to professional life of school staff is covered in the staff/governor acceptable use policy, as well as the staff code of conduct. As with discussion groups, staff are reminded that professional standards should apply to all postings and messages.

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 computing, child on child policies. 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 / 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.

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 other children 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 an 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.

Emerging technologies

The school recognises that technology evolves rapidly. New platforms, applications, games and communication tools will be risk assessed before use in school. Staff will remain vigilant to emerging online risks and adapt curriculum, monitoring and safeguarding arrangements accordingly.

Monitoring arrangements

All staff have a responsibility to identify and report online safety concerns. Concerns should be recorded using a safeguarding concern form or on CPOMS as soon as possible.

The Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSLs) will receive notifications of all online safety concerns. Reports will be reviewed, assessed and acted upon appropriately, with actions recorded and monitored in line with the school's safeguarding procedures.

This policy will be reviewed annually by the Headteacher and presented to the Governing Board for approval. As part of the review process, an annual online safety risk assessment will be undertaken to identify and evaluate current and emerging risks faced by pupils. The findings of this assessment will inform updates to the policy, curriculum, filtering and monitoring arrangements, and wider safeguarding practices. This ensures that the school's approach to online safety remains effective and responsive to changes in technology and online behaviours.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (computers/iPad) and get onto the internet in school I will:
 	
• Ask a teacher or adult if I can do so before using them.
• Only use websites that a teacher or adult has told me or allowed me to use.
• Tell my teacher immediately if:
  ○ I select a website by mistake.
  ○ I receive messages from people I don't know.
  ○ I find anything that may upset or harm me or my friends.
• Use school computers/iPad for school work only.
• Be kind to others and not upset or be rude to them.
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
• Only use the username and password I have been given.
• Try my hardest to remember my username and password.
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
• Save my work on the school network.
• Check with my teacher before I print anything.
• Log off or shut down a computer when I have finished using it.
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer 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 above for pupils using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only. • Only use them when a teacher is present, or with a teacher's permission. • Keep my usernames and passwords safe and not share these with others. • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer. • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. • Always log off or shut down a computer when I've finished working on it. **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. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate. • Log in to the school's network using someone else's details. • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. **Year 5 and 6 only: If I choose to bring a mobile phone into school, I will turn it off and hand it to my class teacher at the start of the day. I will then get the phone back at the end of the day.** **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's 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 above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Old Park Primary School Information Security Policy – Acceptance Form (Teachers)

Please complete and return your acceptance to the School Business Manager

Full name	
Job title	
Contact telephone	

- I have read, understood, and agree to abide by Old Park Primary School's Information Security Policy.
- I understand that this policy may change and that I will read any new versions when I am informed that they are available.
- I further understand that I must read, understand and agree to abide by the acceptable use policies and codes of practice that are relevant to me and that if I have any questions that I may ask the DPO for assistance.

Signed _____ **Date** _____