

Park Road Academy Primary School



**Acceptable Use Policy 2023
- 2024**



Aims of Policy

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- Ensure that pupils benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.
- To give pupils clear guidance on safe and acceptable use of these resources.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and pupils to agree to be responsible users. There are different agreements for staff and children in KS1 and KS2.



Pupils

The Pupil Acceptable Use Agreement at Park Road Academy is known as the Pupil eSafety pledge. This document was created by a group of pupils at the school (known as the Digital Leaders) in collaboration with the Computing Coordinator (J Sidwell).

The pupils designed the pledge using their own knowledge of safe Internet use and conducting research into similar policies used by other schools.

Two versions of the eSafety pledge exist: 'KS1 & LKS2' and 'UKS2'. The difference between the two policies is that UKS2 children must also agree to use email technology safely (a provision not available to younger pupils). Children in our Early Years are equip for a digital life through the Education for a Connective World Framework. This framework describes the knowledge, understanding and skills that children and young people should have the opportunity to develop at different ages and stages. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, how to get support, and what skills they need to be able to navigate it safely.

Children are expected to sign the eSafety pledge along with their parents to show their agreement. They will be expected to sign the pledge at the start of each academic year to allow the pledge to be updated and stay current with the latest technologies.

Please see **Appendix A** for the KS1 & LKS2 eSafety pledge and **Appendix B** for the UKS2 eSafety pledge.

Staff and other volunteers

The Staff Acceptable Use Agreement is in place to ensure that school systems are used in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the systems and other users.

Staff at Park Road Academy are expected to recognise the value of the use of digital technology for enhancing learning and ensure that pupils receive opportunities to gain from the use of digital technology. Staff are also expected to educate the young people in their care in the safe use of digital technology and embed online safety into their own work.

The Staff Acceptable Use Agreement covers the following areas:



- Professional and personal safety online
- Expectations of communications and actions when using school ICT systems • Safe and secure access to technologies

Staff are expected to sign and agree to follow the Staff Acceptable Use Agreement (see **Appendix C**).

Ensuring Internet access is appropriate and safe

In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access has a filtering system which prevents access to material inappropriate for children.
- Children using the internet will be working in the classroom will be under the supervision of an adult at all times.
- Children are educated on how to browse the Internet safely and responsibly.
- Staff will use their professional judgement and check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfE.

A most important element of our Acceptable Use Policy is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children is taken by the class teacher, the Computing Coordinator and the Headteachers. All teaching staff will be made aware of the incident at a Staff Meeting if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.

- 
- If staff or pupils discover unsuitable sites, the Computing Co-ordinator will be informed. The Computing Co-ordinator will report the URL (address) and content to the Internet Service Provider; if it is thought that the material is illegal, after consultation with the ISP, the site will be referred to the Internet Watch Foundation and the police.

Maintaining the security of the school

ICT/Computing network

Security is maintained by updating virus protection and teaching staff are provided with school memory sticks for all school use. Other memory sticks etc. can only be used after consultation with the Headteacher/s and ICT support technician.

The safety and security of the school network is managed by the Local Authority in conjunction with the school's Computing Coordinator.

Using the Internet to enhance learning

Access to the Internet is a planned part of the curriculum that enriches and extends learning activities and is integrated into class schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet are used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other adult) demonstration;
- Pupils may access teacher-prepared materials, rather than the open internet;
- Pupils may be given a suitable web page or a single web site to access;
- Pupils may be provided with lists of relevant suitable web sites to access;
- Pupils are expected to observe the Park Road Academy eSafety Pledge and are informed that checks can and will be made on files held on the system and the sites they access.
- Pupils will be educated in taking responsibility for their own Internet access.

Using information from the Internet:



- Pupils are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non- moderated medium);
- When copying materials from the Web, pupils are taught to observe copyright;
- Pupils are made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using e-mail

Staff and pupils in UKS2 use integrated e-mail systems to communicate with others, to request information and to share information.

- Pupils are only allowed to use e-mail once they have signed and agreed to observe the Park Road Academy eSafety pledge.
- Teachers endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail.
- Pupils may send e-mail as part of planned lessons.
- Pupils are not permitted to use school e-mail systems outside of school.
- Pupils are not permitted to use e-mail at school to arrange to meet someone outside school hours.

Our school web site is intended to:

- Provide accurate, up-to-date information about our school;
- Provide pupils with the opportunity to publish their work on the Internet for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- Celebrate good work;
- Provide parents and other stakeholders with essential up-to-date information;
- Parents can find out more about eSafety and staying safe online by visiting our dedicated eSafety page on the school website (<http://parkroadacademy.co.uk/esafety/>)

- Promote the school.



The point of contact on the web site will be the school address, telephone number and email address. We do not publish pupil's full names or photographs that identify individuals on our web pages without prior parental consent. Home information or individual e-mail identities will not be published. Staff will be identified by their surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

Internet access and home/school links

Parents will be informed in our school information that the pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments by letter, text or email.

Policy written by: L. Taylor

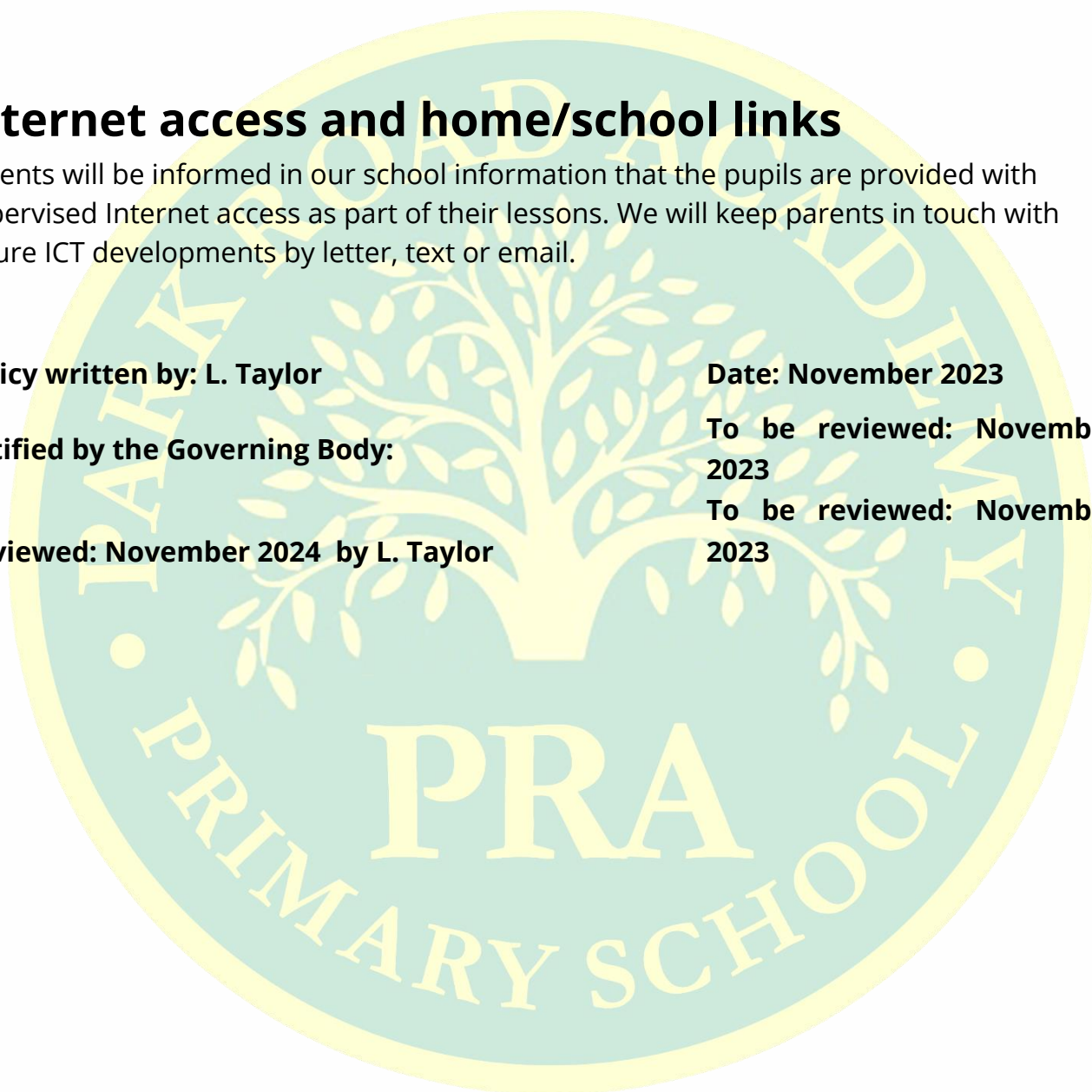
Date: November 2023

Ratified by the Governing Body:

To be reviewed: November 2023

Reviewed: November 2024 by L. Taylor

To be reviewed: November 2023



Appendix A: KS1 & LKS2



Park Road Academy eSafety Pledge



The Park Road Digital Leaders have produced this eSafety pledge to help protect you when using your digital devices and the Internet. It was designed to show you how to behave online and keep yourself safe.

Please read our pledge (and talk about it with your parents) and return the signed form below to show that you agree to follow the pledge.

When you are using the computer:

- Don't make changes to other people's files and folders.
- Keep your files organised with sensible names.
- Respect the school equipment (it's very expensive to replace!)
- Don't use school ICT equipment without permission.

When you are using the Internet:

- Do not search for inappropriate content (ask an adult if you're not sure what inappropriate means).
- Search sensibly (using terms such as 'ks1' or 'for kids').
- Be careful who you communicate with online: people may not be who they say they are.
- Don't arrange to meet up with people over the Internet.
- Don't give out personal information (such as your name, your school, where you live)
- Respect age limits (they're there for a reason!)
- Tell a trusted adult if anything makes me feel sad, scared, or confused.
- If something sounds too good to be true, then it probably is! (Don't click suspicious pop-ups!)
- Keep your password secret and secure.
- Use kind and polite language. (Even though it's on the computer, your words still affect people).
- I understand that my search history can be seen by teachers and other members of staff.

I agree to follow the Park Road Academy eSafety pledge.

Name: _____

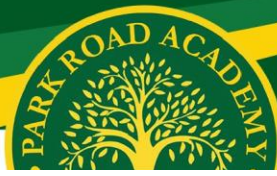
Class: _____

Pupil Signature: _____

Date: _____

Parent Signature: _____

Date: _____



Park Road Academy eSafety Pledge



The Park Road Digital Leaders have produced this eSafety pledge to help protect you when using your digital devices and the Internet. It was designed to show you how to behave online and keep yourself safe.

Please read our pledge (and talk about it with your parents) and return the signed form below to show that you agree to follow the pledge.

When you are using the computer:

- Don't make changes to other people's files and folders.
- Keep your files organised with sensible names.
- Respect the school equipment (it's very expensive to replace!)
- Don't use school ICT equipment without permission.

When you are using the Internet:

- Do not search for inappropriate content (ask an adult if you're not sure what inappropriate means).
- Search sensibly (using terms such as 'ks2' or 'for kids').
- Be careful who you communicate with online: people may not be who they say they are.
- Don't arrange to meet up with people over the Internet.
- Don't give out personal information (such as your name, your school, where you live)
- Respect age limits (they're there for a reason!)
- Tell a trusted adult if anything makes me feel sad, scared, or confused.
- If something sounds too good to be true, then it probably is! (Don't click suspicious pop-ups!)
- Keep your password secret and secure.
- I understand that my search history can be seen by teachers and other members of staff.

When you are using email:

- Don't access your school email outside of school.
- Don't use your email account without permission.
- Ask an adult if you're unsure about opening an email.
- Don't open emails from unknown senders.
- Don't give out personal information over email.
- Use kind and polite language. (Even though it's on the computer, your words still affect people).

I agree to follow the Park Road Academy eSafety pledge.

Name: _____

Class: _____

Pupil Signature: _____

Date: _____

Parent Signature: _____

Date: _____



Device and technology acceptable use agreement for staff and volunteers

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the **headteacher or Designated Safeguarding Lead** in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's **Data Protection Policy** and any other relevant school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems on school devices.
- Share school-related password with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the **headteacher** or **ICT technician**.

- Search for, view, download, upload or transmit any inappropriate material when using the internet.



Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the **headteacher** or IT support.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the **ICT Support**.
- Seek permission from the **headteacher** before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the **ICT Support team**.
- Immediately report any security issues, such as downloading a virus, to the **ICT support team**.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the **ICT Support team** upon the end of my employment at the school.

I will not:

- Not permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the **headteacher**.
- Install any software onto school-owned devices unless instructed to do so by the **headteacher** or **ICT support team**.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices



I will:

- Only use personal devices during out-of-school hours in a the designated area (staffroom), including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours and are locked away in desk draw.
- Only make or receive calls in specific areas, e.g. the staff room unless have permission for emergency use.
- Store all personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Access the school's WiFi using a personal device unless permission to do so has been granted by the **headteacher** or **ICT support team**.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the **headteacher**.

Social media and online professionalism

I will:

- Follow the school's **Social Media Policy**.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:



- Ensure I obtain permission from the **headteacher** and **DPO** before any personal data is transferred from a school-owned device to a personal device.
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure my personal device has been assessed for security by the **DPO** and **ICT support team** before it is used for home.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the **ICT team** and **DPO** to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the **headteacher**.
- Understand that my use of the internet will be monitored by the **ICT team** and recognise the consequences if I breach the terms of this agreement.
- Understand that the **headteacher** may decide to take disciplinary action against me, in accordance with the **Disciplinary Policy and Procedure**, if I breach this agreement.

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	