Pirbright Village Primary School

Online Safety Policy

Contents

Reviewed	Annually
Next Review Date	Summer 2026

a member of Learning Partners academy trust

A member of Learning Partners Academy Trust
A company limited by guarantee, registered in England & Wales, company number 08303773
Registered office: Learning Partners, c/o Guildford County School, Farnham Road, Guildford, Surrey, GU2 4LU.

1. The Role of the DSL

The DSL has overall responsibility for safeguarding and child protection. This includes online safety, and understanding the filtering and monitoring systems, supported appropriately by DSL deputies and the Online Safety Lead.

2. The 4 Areas of Risk

There are 4 main areas that online safety can be categorised into:

Content: being exposed to illegal, inappropriate or harmful content, eg: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users, eg: 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 purpose.

Conduct: online behaviour that increases the likelihood of, or causes, harm; eg: making, sending and receiving explicit images, sharing explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

With the full implementation of the Online Safety Act during spring and summer 2025, online platforms and services are required to assess potential risks to children, and address concerns that arise, particularly around social media. Even if content is not illegal, if it could be considered harmful, or age-inappropriate for children to access, children must be protected from it, by the consistent enforcement of age limits by the platform or service provider.

3. Teaching and Learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils. This is explained to parents in the Online Safety and Agreed Internet Use Form (see appendix) which new parents complete when their child joins the school. Pupils are required to sign an Acceptable Use Policy.

The school internet access is currently provided to Surrey County Council through an RM contract which includes filtering and monitoring appropriate to the age of pupils. The platform used is RM SafetyNet and this monitors an RM recommended filter list as well as a list managed by the school technical support.

Online Safety education is of paramount importance and is taught in every year group through the Computing curriculum and PSHE curriculum. Children are taught what internet use is acceptable and what is not, and given clear objectives for internet use in order to build digital literacy and resilience. Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. They are shown how to publish and present information appropriately to a wider audience.

The school will celebrate Safer Internet Day every year so as to raise whole school awareness of online safety. Parental Online Safety Workshops will be held. Staff and Governors have online safety briefings annually.

The school seeks to ensure that the use of internet-derived materials by staff and by pupils complies with the law, especially copyright law and pupils should be taught to be critically aware of the materials they read. They are shown how to validate information before accepting its accuracy.

Pupils are encouraged and taught how to report inappropriate internet content or misuse to a responsible adult who will pass the information to the Computing coordinator / Online Safety coordinator. They, in turn, will then pass on relevant information to the headteacher, if necessary (in line with the Child Protection Policy).

4. Remote Learning

The school will endeavour to ensure that pupils continue to receive a good level of education by providing a range of resources via our website and learning portal. Parents should be informed of any websites that children will be expected to access by their year group teachers.

We expect pupils to follow the same principles whilst learning at home, as outlined in this policy and agreed by signing the letter 'Online Safety and Internet Use' (Appendix).

Children may be contacted by their year group teachers and learning support assistants via our online learning platform (tapestry), via email or via Teams. If the school chooses to communicate with pupils via Teams, then pupils must uphold the same level of behavioural expectations as they would in a normal classroom setting.

Any significant behavioural issues occurring on any virtual platform should be recorded and an appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using normal restorative approaches.

Staff should be mindful that when dealing with any behavioural incidents online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

5. Managing Internet Access

School ICT systems security will be reviewed regularly by the Computing coordinator and ICT Support. Virus protection will be updated regularly and security strategies will be discussed with the Local Authority.

In the vast majority of cases, children use internet with a supervising adult. However, as children progress through the school and their use of the internet increases with independent learning, extended research projects and opportunities to use mobile technologies to enhance their learning; it is important that we provide opportunities for them to use this resource independently. This approach is carefully monitored and only works as the children progress up the school with an excellent understanding of the internet and online safety, and with appropriate filtering in place. We are seeking to develop pupils as good 'Digital Citizens' and we encourage the development of 'digital resilience' – where they know how to minimise risk online and report any concerns.

Appropriate sanctions are used if pupils do not use the internet properly.

6. Email and Social Media

Email is taught as part of our Computing curriculum. Pupils may only use approved e-mail accounts on the school system and must immediately tell a teacher if they receive offensive email whilst in school. Pupils are taught not to reveal personal details of themselves or others in email communication, or arrange to meet anyone. They are also taught that the opening of mail from unknown senders should be considered carefully in each case and attachments not opened unless the sender is known.

Staff to pupil and parent email communication must only take place via a school email address and will be monitored. If any disclosures relating to a child protection issue are made through this line of communication, they must be raised immediately with the school DSL. The school will carefully monitor email from pupils to external bodies and this will only be facilitated through curriculum sessions.

Pupils will be taught to consider carefully anything they write and will be educated in the impact of cyberbullying / online bullying. If a child discloses to a member of staff that they have received any offensive or concerning email this will be passed onto the Computing coordinator / Online-safety coordinator who will inform the headteacher and appropriate discussion with the children, parents / carers will take place.

Children should not make use of social networking sites / chatrooms in school unless their specific use is approved and pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils are advised that the age restriction for using various different social media platforms is from 13+, with some (such as YouTube) being 18+. Pupils are taught about the potential dangers and pitfalls of using social media and the importance of managing privacy settings and considering carefully what they post. Pupils are advised to use nicknames and avatars when using age-appropriate social networking sites outside of school. Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils, and parents and carers are informed that if they take photos or video images of children during school events, they should not publish these images in the public domain.

If children do access age inappropriate social media platforms at home and issues concerning this are brought into school, the school will deal with any incidents according to our Safeguarding Policy. A senior teacher will investigate the incident with the children concerned and communicate with parents appropriately.

The school uses a Twitter and an Instagram account, which are controlled by the staff with the authority of the head teacher in order to communicate with the school community.

In all Social Media, staff will not 'friend' children, and should block children who attempt to follow them. The school email addresses and social media accounts are acceptable contact points.

7. Unsuitable/Inappropriate activities

Sexual harassment and harmful sexual behaviours (unwanted contact of a sexual nature) can occur online as well as offline. Online sexual harassment, which might include sexting – the non-consensual sharing of sexual images and videos and sharing sexual images and videos. This includes inappropriate sexual comments on social media; exploitation; coercion and threats. Safeguarding issues that can manifest themselves via peer on peer abuse will include issues such as these, and will be dealt with according to our Antibullying, Behaviour and Safeguarding policies.

8. Published content

School Website

The school website includes all information as required by law, following guidance for educational settings https://www.npsa.gov.uk/resources/smc-guidance-educational-settings.

. The contact details on the website should be the school address, e-mail and telephone number and a main contact person. Staff or pupils' personal information will not be published. The headteacher takes overall editorial responsibility to ensure that content is accurate and appropriate.

Pupils' images and work

Photographs that include pupils will be selected carefully and full names will not be used on the website.

Permission from parents or carers is attained on admission (unless a parent has elected to withdraw their child) to allow photographs of pupils to be published on the school website. A record of those children who do not have permission is kept by the school. Parents are clearly informed on the admission form of the school policy on image taking and publishing.

9. Managing filtering and Monitoring

There are many reasons why filtering and monitoring are required and whilst we have a duty to ensure that appropriate filtering and monitoring are in place, we should be careful to ensure that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught. In school the purpose is to ensure that children do not access unsuitable or inappropriate content. One example is around radicalisation. The Prevent Duty is a statutory obligation for schools to keep children safe from the risk of radicalisation and extremism. The school uses a central filtering system provided by RM (who provide our internet service). Using RM SafetyNet, and a combination of RM recommended filter lists, and lists that we manage, we are able to filter and monitor online activity. Alerts triggered by RM SafetyNet are passed to the DSL and any necessary action taken. We are responsible for informing RM of any concerning sites that are not currently filtered. We are able to override some filters if we consider certain websites to be of value to teachers or the curriculum, e.g. Google images, YouTube and Pinterest. All use of the internet must adhere to the school's Acceptable Use policy. If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing coordinator. The Computing coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable: safeguarding risks will be considered and responded to in consultation with the DSL.

10. Managing emerging technologies

The school is actively interested in emerging technologies. We recognise the need for us to educate our pupils in the use of all forms of technology, not only for use in school but also to facilitate their life beyond school. Emerging technologies are examined for educational benefit and potential risks assessed by the SLT before use in school is allowed. The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

These risks reflect situations in the off-line world, and can be encountered at home as well as in school. Therefore, if any issues concerning emerging technologies are brought into school, the school will deal with them according to our Online-Safety policy, in conjunction with our Antibullying, Behaviour and Safeguarding policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

11. Managing personal devices

Personal mobile phones and associated cameras will not be used during lessons or formal school time. Pupils must hand in their personal devices (switched off) for safe keeping during the school day. The sending of abusive or inappropriate text messages is forbidden. Pupils will be carefully supervised during any curriculum video conference calls. Any mobile technologies (iPad / iPod) used for recording or assessing in school will be closely monitored and will remain in school. Smart watches should not be brought into school. The use of fitness trackers should be limited to monitoring activity, and they should not be receiving updates throughout the day. Use of fitness trackers in lessons should be agreed by the teacher in charge on a case by case basis.

Staff, visitors, volunteers or governors must not show, share or record images with children on personal devices. Adult use of personal devices is not permitted during lessons, and no member of staff will use a personal device to record any child. In EYFS settings, it is important that all personal devices with a camera be disabled during school hours.

12. Protecting personal data

Storage of all personal data within the school and online, will conform to the General Data Protection Regulation 2018.

13. Authorising Internet access

All staff and school governors must read and sign the Acceptable Use Policy before using any school computing resource. The school will maintain a current record of all staff and pupils who are granted access to school computing systems. Any person not directly employed by the school will be asked to sign a copy of the Acceptable Use Policy before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.

The school will annually audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

14. Handling Online Safety complaints

Complaints of internet misuse will be dealt with by the Online Safety coordinator.

- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and be brought to the attention of the DSL immediately.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the internet.

15. Communication

Community use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the school Online Safety policy.

Introducing the Online Safety policy to pupils

Appropriate elements of the Online Safety policy will be shared with pupils:

- Online-safety rules will be posted in all classrooms.
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils.

Staff and the Online Safety policy

All staff will agree to the Online Safety policy and have its importance explained.

- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting Parents' Support

Parents' and carers' attention will be drawn to the Online Safety policy in newsletters and on the school website. They will regularly be provided with additional information on Online Safety.

Parents will also sign an 'Online Safety and Agreed Internet Use' form upon entrance of their child to the school which details the partnership needed in keeping our children safe; the role they play in maintaining the school's reputation; our policy on the use of photographs from school events'; and the responsible use of social media.

Appendix

Letter given to parents as their child joins the school:

Online Safety and Internet Use

Dear Parents,

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Internet use is an important part of the curriculum and a necessary tool for staff and pupils.

Our school responsibilities and philosophy

Here at Pirbright, we understand how important it is to work in partnership with you, as parents, to develop our children into thoughtful and sensible 'digital citizens'. To that end, we advocate the 'ABC of Internet Use':

Awareness – We have a progressive and broad online safety curriculum taught as part of computing lessons, through PSHE units and across the curriculum. The children are taught how to use the internet wisely, the potential issues they may confront and how to deal with any concerns.

Boundaries – We have a filtering system in place which protects the children from most inappropriate online content.* We monitor this system continually and adapt it as necessary. We also put restrictions on mobile devices to further protect the children. We have acceptable use policies for both adults and children.

Communication – It is a vital part of our culture that children talk to us about concerns they have or issues that arise as they use the internet. Also, we aim to support you, as parents, in promoting safe use of the internet and devices at home.

Ultimately, we encourage the development of 'digital resilience' – where children know how to minimise risks online and where they report any concerns to an adult.

**The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access. The school will annually audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective. (The Online Safety Policy is available, in full, on the school website.)*

Your responsibilities in partnership with the school

We would ask that you support the school in the following ways:

- Read through online safety information on the school website or distributed regularly by the school and talk through the documents with your child.
- Put in place appropriate filtering and blocks on your child's mobile devices, gaming devices and home laptops / PCs.
- If possible, attend parent information sessions relating to online safety as they arise on the school calendar.
- Follow the school's requests as to when and where you can safely take photographs during school events and ensure that images are only for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.
- Support your child's school in your own online communications, considering the long term effects of negativity to a school's reputation in a digital world – please speak to us about any concerns or disputes rather than posting your comments online.

✂ I have read the 'Online Safety and Internet Use' document. I give permission for my child _____ to use the internet in school and I am satisfied that the school will do everything they can to promote safe internet use.

I will work in partnership with the school to educate my child in safe use of the internet and will ensure that I support the school in all online communication.

Signed _____ Date _____