Perryfields Primary School

Online Policy

Author:	David Harris/Dean Spittle	**Date:** 30.1.26
Last Reviewed on:	February 2026	
Next review due by:	February 2028	

Introduction

At Perryfields Primary School, we understand the responsibility we have to educate our pupils, parents and carers about online safety.

Our aim is to give all children the skills to remain both safe and legal when using the internet and related technologies.

Perryfields Primary School has a whole school approach to online safety, which include:

1. an effective range of technological tools
2. policies and procedures, with clear roles and responsibilities
3. a comprehensive online safety programme for pupils, staff and parents.

This policy is to be read in conjunction with all other policies particularly: Remote Learning Policy, Child Protection Policy and Photography and Video Policy.

Artificial Intelligence (AI) tools are increasingly embedded within online platforms, applications and services accessed by children and adults. Perryfields Primary School recognises the potential benefits and risks associated with AI and is committed to ensuring that its use supports safeguarding, online safety and data protection requirements in line with current statutory guidance, including Keeping Children Safe in Education (2025).

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership at Perryfields Primary School. All staff have received CEOP (Child Exploitation and Online Protection) training. The Head Teacher has overall responsibility supported by the Lead for Computing and members of the Safeguarding Team. All concerns will be recorded using the CPOMS template by the member of staff who has directly dealt with the incident/situation. Once dealt with, the relevant information and action taken is entered into the system by a member of the Safeguarding Team.

It is the role of the Head teacher, Designated Safeguarding Leads and Lead for Computing to keep up-to-date with current issues and guidance through organisations such as:

- CEOP
- Child Net
- Thinkyouknow
- Internet matters
- Pegi
- NSPCC
- Internet watch foundation

The Head teacher will ensure all staff and Governors are updated as necessary and complete any necessary training.

All teachers and support staff will promote online safety as part of their day-to-day responsibilities.

Staff will receive regular online safety updates annually and as and when emergent guidance becomes available between the annual updates.

Parents will be offered online safety workshops, online safety guides and be informed of any online safety issues that need addressing (see Online Safety Complaints/Incidents).

Curriculum

We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. Online safety posters will be prominently displayed in both the hall and Computing Suite and referred to regularly.

Computing and online resources are increasingly used across the curriculum. We will ensure online safety guidance is given to the pupils on a regular and meaningful basis. All opportunities, within a range of curriculum areas are used to teach online safety and will educate pupils about the dangers of all technologies. Opportunities are given to develop Digital Literacy and digital resilience and are taught as part of the curriculum.

As part of the school's approach to online safety, pupils are taught age-appropriate awareness of Artificial Intelligence (AI). This includes understanding that AI-generated content is computer-produced, may not always be accurate, reliable or appropriate, and should not be trusted without adult guidance. Pupils are reminded not to share personal information online and are encouraged to report any content, including AI-generated material, that causes concern, confusion or discomfort to a trusted adult.

The Jigsaw scheme of work (PSHE) and One Decision provides the children with an awareness of online bullying. All children know how to seek help if they are affected by these issues. Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the computing curriculum.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it an invaluable resource for education as well as a potential risk to young people. Students will only have supervised access to internet resources through the school's fixed and mobile internet technology. Staff will preview any recommended sites, YouTube clips and other photographs and video clips before use. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research. Our internet access is controlled through SIPS education. Staff and pupils are aware that school based email and internet activity is monitored and explored further if required. If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the Lead for Computing who will instruct SIPS to block future access to that page. The school delegates its responsibility to SIPS education to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Where AI-based tools or platforms are used to support learning, access will be supervised and controlled by staff. Staff will ensure that any AI-generated content used with pupils is appropriate, accurate and suitable for their age and stage of development. Pupils will not be permitted to access open or unrestricted AI tools independently.

Security and Data Protection

The school and all staff members will comply with the General Data Protection Regulations Act (May 2018). Password security is of paramount importance for all staff, particularly as they are able to access and use pupil data. Staff will have secure passwords, which are not shared with anyone. The system is configured to require passwords are changed on a regular basis. All users read and sign an Acceptable Use Agreement to demonstrate that

they have understood the school's Online Safety Policy prior to gaining access to the school's systems. This is overseen by the Lead for Computing on an annual basis.

In line with safeguarding and data protection requirements, staff must not input personal, sensitive or identifiable information relating to pupils, families or staff into Artificial Intelligence (AI) tools. Any use of AI by staff must comply with the General Data Protection Regulations and the school's data protection and safeguarding policies.

Online Safety Complaints/Incidents

As a school, we take all precautions to ensure online safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. All complaints should be made to the Head Teacher. Incidents will be logged and reported to the FGB via the Head Teacher's termly report. It is important that the school work in partnership with pupils and parents to educate them about stranger danger, cyber bullying etc. Children, staff and families need to know what to do if they or anyone they know are a victim of cyber bullying. All bullying incidents will be recorded and investigated. These incidents will be recorded using SIMS.

Mobile phones

Children are permitted to bring phones to school when they are in Y6 and walk home (usually after Easter, unless agreed by the Headteacher); however, they will be handed into the office on entering school and picked up at the end of the school day. Staff are permitted to have phones in school. These are to be locked in a classroom cupboard or filing cabinet when working with the children. They are not to be used to photograph or record the children for any reason (Refer to Use of Mobile Phones and Camera Policy).

Commitment to Parents

We provide online safety workshops for parents throughout the school year. This provides parents with an awareness and understanding of safety measures, which can be put in place at home. Staff also highlight the importance of online safety as part of the curriculum expectations meetings in the summer term.

Review of Policy

There are on-going opportunities for staff, children and families to discuss online safety concerns with our safeguarding staff. This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated. Particularly Data Protection Act 2018.

Appendix

1. Primary Pupil Acceptable Use of Information Technology Agreement/Online Safety Rules
2. Staff, Governor and Visitor Acceptable Use Agreement

Appendix 1

Primary Pupil Acceptable Use of Information Technology Agreement/Online Safety Rules

- I will only use Information Technology (IT) in school for school purposes.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or IT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- I will make sure that all contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- I will not give out my own details such as my name, school, phone number or home address.
- I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I know that the school will check my use of IT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my online safety.

Name _____ Class _____

Signed (child)_____

Signed (Parent) _____

Appendix 2

Perryfields Primary School

Acceptable Use of IT Agreement Staff, Governor and Visitors

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or Governing Board.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or Governing Body.
- I understand that Artificial Intelligence (AI) tools may be used to support professional tasks; however, I will not upload personal, sensitive or identifiable data and will apply professional judgement to ensure that any AI-generated content is accurate, appropriate, unbiased and suitable for use in school.
- I will not use or install any hardware or software without permission from the e-safety co-ordinators.
- I will only use the encrypted USB Memory Stick issued by school.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or headteacher.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school (including via social media), will not bring my professional role into disrepute.
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will ensure that only children whose parents have given permission for them to use the Internet and IT are enabled to do so at school.
- I agree to follow this code of conduct and to support the safe use of IT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Job title: ……..

Commented [DH1]: No longer relevant – T Drive