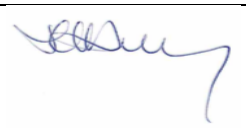
RISE PARK PRIMARY AND NURSERY SCHOOL

E-Safety Policy

March 2026

Signed by Chair of Committee	
Print Name	Jeanette Kirkby
Date	March 2026
Date of next review	March 2028

Contents

E-Safety Policy

1 Introduction

1.1 This policy applies to the whole school including the EYFS and all teaching and support staff.

Policies and documents that support the e-safety policy in school:

- Computing policy
- Safeguarding
- Behaviour policy
- Acceptable Use Policy (A.U.P.) for staff and pupils

2 Teaching and Learning

2.1 The school has a duty to provide pupils with high-quality internet access as part of their learning experience in school, and to prepare them to make safe and effective use of such technologies outside of school.

2.2 The internet, along with the digital communications afforded by it, are important because:

- The internet is an essential element of 21st century life for education, business and social interaction.
- Internet use is a part of the statutory curriculum and is a necessary learning tool for staff and pupils.
- Internet and digital communications enhance and extend learning opportunities for all pupils.

2.3 We can minimise risk to staff and pupils by:

- Designing internet access expressly for student use that will include filtering and monitoring of content only appropriate to the age of students.
- Setting clear boundaries for the appropriate use of the internet and digital communications. These boundaries will be discussed with both staff and pupils, and a home-school internet agreement will be signed by all parents and children at the start of a new school year.
- Ensuring that all pupils are e-safety aware from EYFS onwards, and that the key principles of online safety and digital citizenship are revisited at the start of **any** lesson, from any subject area, where digital technologies are going to be used.
- Making explicit links with the JIGSAW scheme of work used to teach PSHE throughout school, especially in sessions which deal with issues related to online safety. Any issues related to 'real world' identity, citizenship or peer-on-peer abuse which are covered through the scheme should also have their digital parallels made clear to the children.
- Continuous provision and education of current topics in online / e-safety through the use of the ProjectEVOLVE schemes of work. The scheme, embedded in school since 2022, will be used all year long, from EYFS to Year 6, to ensure that all children receive high quality online safety teaching that is age and content specific.
- Ensuring children only use computers when signed in with their unique, secure logins in KS2, and their year group logins (KS1). On iPads, ensuring that children in all classes are 'assigned' a numbered iPad so that any instances of inappropriate use can be effectively traces.
- Ensuring pupils are not left unsupervised using Computing equipment.
- Ensuring that the following statement is added to the bottom of any homework or home-learning task that involves researching information or looking up a recommended website:

  "*Always ask a known and responsible adult before using the computer; make sure your known and responsible adult finds the exact site you want to use before you start your work. Always remember the* internet *Safety considerations that you are taught in school."*

2.4 Our I.T. support, which is currently provided by Schools I.T., aims to keep our system safe and secure by:

- Reviewing the school ICT system security regularly.
- Updating all security software regularly.
- Discussing security strategies annually with the ICT subject leader, governor for ICT and Senior Leadership Team.
- Working in partnership with IT services to ensure filtering and monitoring systems are in place to protect pupils, and that these are reviewed and improved.
- Regularly checking that the filtering methods selected are appropriate, effective and reasonable.
- Filtering and monitoring software deployed by the school can send instant notifications to DSLs / Safeguarding Leads when specific devices are used to search for / gain access to blocked content. This feature is discussed in more detail in the school's Safeguarding Policy document.
- Ensuring that staff online access is kept safe & secure through the use of custom two-factor authentication through Office 365.
- Prompting staff to changed their login details for computer and Office 365 on a timely basis.

2.5 E-mail – There is currently no internal e-mail system available for use by pupils, and the e-mail system used by staff, Office 365/Outlook, is not accessible from any devices used by pupils.

3 Pupil Use / Content Related to Pupils

3.1 Pupils will be taught to:

- Immediately tell a teacher if they receive something upsetting or inappropriate when using a computer or internet -linked device whilst at school.
- Not reveal their personal details or those of others, or arrange to meet anyone without specific permission or accompaniment from a known and trusted adult.
- Treat incoming e-mails as suspicious and that attachments should not be opened unless the author / sender of the e-mail is known. Topics covered through ProjectEVOLVE lessons, and JIGSAW PSHE deal with these issues in greater detail.

3.2 Published content and the school web site:

- Staff or pupil personal contact information will not be published. Any contact details given online should be those of the school office, and personal staff e-mails should <u>never</u> be given out to parents, carers or pupils unless express consent has been obtained from that staff member beforehand.
- Written permission from parents or carers is obtained when pupils join the school, before work or photographs of pupils are published on the school website or in any other medium.
- The Head teacher or a nominated individual will take overall editorial responsibility and ensure that published content on the school website or social media accounts is accurate and appropriate.
- Parents grant written permission for their child's image to be published on the school website, on the school's Arbor platform and in newsletters in print and digital. Staff check the permissions list before uploading images.
- Without this permission, children's images will not be used in any way. Photographic consent forms are always sent out at the start of each new school year, to ensure that any changes in circumstance in regards to this issue are accurately reflected in the school's records.
- Parents are also regularly asked whether these permissions have changed throughout the course of the school year, and any relevant changes are then made to the whole-school permissions list. This is then shared with staff members immediately so that they are aware of the changes that may have been made.
- Parents/pupils are informed not to take/share online images of other children onto the internet at all school events which they may attend, such as open mornings, Christmas productions and Sports Days. Rise Park is proactive in photographing school events in house (with knowledge of which children have what permissions, to share photos safely with families and in school communications).

3.3 Social Networking and personal publishing – we do not allow pupils to use or access social networking sites but know that these sites may be accessed at home. With this in mind pupils will be given e-safety guidance on safe internet use both in and out of school and this will include:

- To never to give out personal details of any kind which may identify them, their family members, their friends or their location.
- To not place personal photos on any social network space without considering how the photo could be used either now or in the future.
- To only invite known friends and deny access to others when using social networking and instant messaging services.
- Being advised on internet security and to be encouraged to set complex passwords; to deny access to unknown individuals and to block and report unwanted communications to a known and trusted adult or individual.
- Parents, carers and pupils should be routinely reminded that the minimum age for having a personal account on any social media platform is 13 years old (or higher). This information is frequently circulated to parents and carers on the newsletter, and will be included as part of the e-safety agreement that they are asked to sign alongside their children at the start of the new school year.

4 Health and Safety / Safeguarding

4.1 Radicalisation and Extremism - We recognise the risk of online radicalisation through the use of the internet and social media. To combat this, we use a Local Authority approved filtering system, which blocks sites with inappropriate content, including extremist content.

4.2 Policy decisions authorising internet access:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material will *never* appear on a computer connected to the school network.
- The school cannot accept liability for any material accessed, or any consequences of internet access, although it will do all that is possible to reduce the risk of inappropriate material being accessed.
- The e-safety coordinator and technician will monitor the network regularly to establish that the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

5 Communicating e-Safety

5.1 We will ensure pupils are e-safety aware by:

- Informing pupils that the school network and internet use will be monitored.
- Delivering a programme of training in e-safety which will be developed and delivered making use of appropriate materials. This is taught through the ProjectEVOLVE Schemes of Work for Computing which have been taught in school since September 2022. These resources are selected to ensure progression across school and are adapted by teachers to better meet the needs of their classes.
- This will further be supported by lessons taught as part of the JIGSAW scheme of work in specific year groups which deal with issues around e-safety and the principles of being a good digital citizen.
- Ensuring pupils have read and signed the pupil A.U.P. Those pupils who have not should not be allowed unsupervised access to the internet until the aforementioned document has been returned.

5.2. We will ensure that staff and governors are e-safety aware by:

- Giving a copy of the school's e-safety Policy to relevant adults and explaining its importance.
- Informing staff that the network and internet traffic can be monitored and traced to the individual user.
- Explaining that those managing filtering systems or monitoring ICT work have clear procedures for reporting issues under the supervision of the S.L.T.
- Ensuring staff understand that telephone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship in any discourse they have with parents, carers and pupils.
- Ensuring new staff are familiar with the e-safety policy and procedures
- Ensuring staff have read and signed the Staff A.U.P.

5.3 We enlist the support of Parents and Carers by:

- Drawing parents and carers attention to the School e-Safety Policy in newsletters, the school brochure, on the school website and through any other relevant correspondence that may be sent out to families.
- Providing parents and carers with current and up-to-date advice on e-safety issues, including through the use of online safety / e-safety homework projects, as and when relevant.
- Keeping regular contact with parents and carers through an internet safety section on the school newsletter, published monthly.
- Maintaining a selection of e-safety resources for parents and carers to access. These are available from the school office, with other copies being available upon request.
- Ensuring that parents and carers sign and return a consent form based on part of the pupil A.U.P.

5.4 Handling e-safety complaints:

- Complaints of internet misuse will be referred to the e-safety coordinator.
- Any complaint about staff misuse will be referred directly to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures and referred to one of the school's D.S.L.'s (Designated Senior Leads)
- Any incidents of child-on-child abuse that occur online should be treated in exactly the same manner as those that occur offline, with staff following the same procedures in accordance with the whole school behaviour policy. Any such incidents should also be recorded in the class behaviour/reflection book, or logged using MyConcern depending on the severity of the abuse, so that a permanent record of what has occurred remains available and can be tracked in the future if necessary.

6 Filtering and Monitoring

Online Safety (Keeping children Safe in Education, 2025 Page 37 - 42 Paragraphs 132 – 151)

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

When children use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. We acknowledge that many pupils may have access to the internet using their own devices and therefore our wider curriculum and linked policies (for example mobile phone policy) ensure that pupils have an awareness and understanding of online risks.

Governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness (Keeping Children Safe in Education, 2025 Page 40, Paragraphs 140 – 143;) with clear identified role and responsibilities for all involved in this area of safeguarding.

At Rise Park Primary and Nursery School we ensure that we meet the Digital and Technology Standards as detailed in the DFE publication 'Meeting digital and technology standards in schools' (23 March 2022, updated 12 February 2026) Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - GOV.UK (www.gov.uk)

If artificial intelligence (AI) tools are used within school, they should meet guidance outlined in DFE publication 'Generative AI: product safety standards' (Updated 19 January 2026)

The monitoring of all issues related to e-safety at school is the primary responsibility of the e-safety officer / Computing subject leader and the school's Senior Leadership Team.

6.2 Review: This policy will be reviewed every two years.

Mr S Berry *Computing Curriculum Lead* *March 2026*