E-Safety Policy

Originator	**Jon Lidbetter**
Issue Date	**February 2024**
Agreed by staff	**February 2024**
Ratified by Governors	**March 2024**
Signed	
Date	
To be reviewed	**February 2025**
Monitored by	**Head Teachers and Curriculum & Standards**

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

The E-Safety Policy relates to other policies including those for Computing and for child protection.

Introduction

Race Leys Infant School views the matter of E-Safety collaboratively with child protection. All staff and pupils have a duty of care to be aware and vigilant of their own and others e-safety at all times. This policy should be read alongside the child protection policy, acceptable use policy and social network policy.

Roles and responsibilities

Governors will view and agree to all policies before they are published.
The Head teacher will have overall responsibility for all e-safety matters and will be informed of all incidents in line with the reporting sheet used for recording and reporting e-safety incidents.
The E-Safety Co-ordinator will ensure the E-Safety policy is updated annually and current practice falls in line with the stated guidelines.
All staff have a responsibility to support E-Safety practices in schools. Pupils and staff at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach E-Safety protocols or those laid out in the Acceptable Use Policy.

Aims

1.1 General Aims of Race Leys Infant School

At Race Leys Infant School we strive to create an atmosphere that is happy, caring and challenging. We want every child to feel they belong here and to feel safe and secure. We believe in the importance of developing the whole child through offering a broad, balanced and creative curriculum where both individuality and team-work are valued. We will help our children to begin to develop learning skills that will last a lifetime, so that they can make their best contribution to the community and society.

With regard to E-safety, we will ensure:

- pupils know how to communicate safety and respectfully online, keeping personal information private, and can recognise common uses of information technology beyond school;
- a continued development of self-assessment of e-safety using the 360° tool.
- staff are provided with online safety training to ensure they understand their expectations, roles and responsibilities.

1.2 Aims of E-safety

The requirement to raise awareness in children and young people of the risks associated with inappropriate contact via the internet and content on the internet is addressed as part of the wider duty of care to which all teachers are bound. It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies. This may be as discrete internet safety lessons as part of the Computing curriculum, delivered via whole school assemblies or embedded within all curriculum work wherever it is relevant. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe pupil use.

- In line with 'Every Child Matters - Staying Safe' we will raise awareness of children and adults to the risks associated with use of the internet and other electronic communications and how they can protect themselves. This protective behaviour will be integrated into the curriculum.

- The internet is an essential element in 21st century life for education, business and social interaction. The school will provide students with quality internet access as part of their learning experience.
- Internet use will be a part of the statutory curriculum and will be used as a necessary tool for staff and pupils.
- The E-safety Policy will work alongside and will cross reference with the Safeguarding Policy.

Teaching and Learning

2.1 Overview of E-safety Curriculum

In line with National Computing Curriculum, 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.

In line with the Race Leys Infant School E-safety curriculum, pupils will -

- Build on existing skills and knowledge
- Access age appropriate use of the internet
- Be taught appropriate and acceptable internet use through modelling and discussions
- Use the internet to enhance cross curricular experiences
- Learn how to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Managing Internet Access

3.1 System Security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-safety issues will be recorded and dealt with immediately.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its partnership with Warwickshire ICT Development Services.
- Warwickshire ICT Development Services also filter and monitor internet usage within school and immediately flag up any concerns regarding internet searches, use of key words within searches and computer usage.

3.2. Accessing the Internet

- Each classroom has access to the internet via an interactive whiteboard. We also have 30 Laptops, 15 Toshiba mini laptops and 16 ipads and several control devices. We have also purchased an additional set of iPads for class use and each class teacher will have an iPad to use within school. The LA monitors the websites visited and the user's activity.

3.3 Reporting concerns

3.3.1 Reporting system for staff

- Reporting forms (attached to this policy) are available in all rooms around the school and will be completed by any member of staff if they have a concern about the safety of any child using the internet, at school or home. This includes the sending or receiving of emails to / from the children.
- Reporting forms will be completed immediately and contain as much fact and detail as possible. All staff have had Safeguarding Training which includes the completion of these forms.
- On completion they will be passed to a Designated Safeguarding Lead (DSL) who will then follow the school reporting procedure.
- The Warwickshire ICT Development Service will be informed over the phone if the incident involves a website/ image / email etc whilst at school.
- The governors will be made aware of all reports made.
- The E-safety Policy and E-safety Curriculum will be changed and adapted to suit the needs highlighted by reports made.
-

3.3.2 Reporting system for pupils

- All pupils are encouraged to talk to adults if they ever feel unsafe on the internet. They are taught the 'Zip It, Block It, Flag It' system and encouraged to follow its guidelines.
- E-safety posters are displayed in all classrooms.
- PSHE Protective Behaviours unit works with children in developing a communication hand, highlighting people each child would feel comfortable talking to if they felt their 'Early Warning Signs'. Children are reminded of this during E-safety assemblies/ lessons.
- Our Computing Curriculum uses Purple Mash which incorporates required areas of E-Safety curriculum. All teachers are aware of and use the 'Education for a Connected World' framework to support their planning. This has been customised to show skill progression and coverage across all year groups.

3.4 E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail. These will be dealt with by the class teacher and head teacher and also the Safeguarding Team if necessary.
- Pupils must not reveal personal details of themselves or others, other than authorised information in e-mail communication, or arrange to meet anyone without specific permission. This is taught throughout the year via assemblies, room displays and ICT lessons.
- Whole-class email addresses will be used.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Members are to use their professional conduct when using the schools e-mail account system.
- Parents do not have access to staff email addresses. They are able to email their child's teacher using Edulink. Emails between staff and parents using Edulink are forwarded by admin for complete transparency.

3.5 Photographing and Videoing

- All photographs and videos will be taken on school devices. If such equipment is being taken off the premises e.g. on an external trip, all existing content will be removed before leaving the school site.
- All photographs and videos will not be stored on memory sticks or laptops which are leaving the school site, unless such devices are encrypted.
- Photographs and videos will only be taken of children whose parents have given signed permission. Such signed documents will remain on file for the duration of the child's time at Race Leys Infant School.
- Photos and videos of children will include groups and not individuals and will always show the intended learning context.
- Photos and videos of children who have left the school will be deleted and removed from the desktop computers.

3.6 Published content

3.6.1 School web site, FACEBOOK and TWITTER

- The contact details on the Web site and social media platforms should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

3.6.2 Digital Signage

- No personal information will be published. If names are used it will only show first names and the year group or class name where needed for clarification e.g. in the instance of two children sharing the same name.

3.6.3 Publishing pupil's images and work

- Images of children and their work will be published on our school website and the school Facebook and/or Twitter page. Written permission from parents or carers will be obtained before photographs of pupils or images of work are published.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified and will show pupils in their intended learning context.
- Pupils' full names will not be used anywhere, particularly in association with photographs.
- No personal details will accompany published photographs or videos e.g. children's names, age.

3.7 Social Networking and personal publishing

- Social networking sites and newsgroups will be blocked in school unless a specific use is approved.
- Throughout the academic year pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Pupils are taught of the possible risks involved with online gaming e.g. communicating with unknown people, sending or receiving files.
- Parents are asked to not publish any photos or videos taken when on the school site on any social networking sites. In the case of these guidelines not being followed appropriate action from the Head teacher will be implemented.
- Members of staff wishing to be involved in social networking sites outside of school will do so using their professional conduct.
- Any child under the age of 13 known to have a social network account will be reported through the appropriate channels.

3.8 Management

3.8.1 Filtering

- The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the class teacher, school E-safety coordinator and Head teacher.
- The E-Safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.8.2 Managing video conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.

3.8.3 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The LA and Governors will be consulted when deciding on which emerging technologies to purchase. All new technologies and software will aid the teaching and learning of pupils.
- Staff and pupil mobile phones will not be used during lessons or formal school time and will not be used to photograph or video children. Mobile phones will be kept in a locker during lesson time and are only to be used in the staffroom.

3.9 Mobile devices

The school embraces the use of mobile technologies in school by both staff and pupils.

- **3.9.1 School owned mobile devices at home**
- School owned mobile devices are available for staff to take home to support work done outside of school hours. They will be used for school tasks only.
- Internet use on these devices will be monitored when in school, sites visited at home will be flagged when on the school site and will be reported if inappropriate.
- Personal pupil information will be stored on encrypted devices ONLY if it is to be taken off the school site.
- Photographs and videos will regularly be removed from mobile devices and stored on the school secure shared system.
- School devices will not be used for personal use in school or at home

3.9.2 Personal mobile devices in school

- All personal devices will remain in a secure lockable cabinet during school hours.
- They will not be used to take videos or photographs during school hours.
- Mobile phones may only be used in the staff room during lunch times.

3.10 Cyber Bullying

Cyber bullying is not and will not be accepted by any member of Race Leys Infant School.

- All pupils are taught the expectations and sanctions of cyber bullying.
- All staff and pupils are aware of the reporting process they should follow if they become aware of cyber bullying.
- Any pupil found to be involved in sending any form of cyber bullying, to other RLIS members or externally, will have internet privileges removed.

3.11 Data Protection & Filtering

- Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018.
- All internet content will be continuously monitored and filtered by the LA with any issues flagged to the Head Teacher.
- All members of staff will continuously monitor and filter the use of internet during lessons and when mobile devices are used in the classroom, following the suitable reporting of inappropriate websites process if needed.

3.12 Passwords

- All governors, teachers, TA's, support staff and pupils are provided with a secure password, gaining them access to the school system and the Learning Platform.
- Adults in school are responsible for the security of their own passwords and area. They will keep them private and ensure devices are re-locked when not in use to ensure positive security of personal details.
- Pupils and staff passwords can be changed by request to the E-safety Co-ordinator.
- Pupils log in details may be printed in order to support their use during lessons but will be stored securely when not in use.

Policy Decisions

4.1 Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the acceptable ICT use agreement, 'E-Safety Agreement Form for School Staff', before using any school ICT resource.
- Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return an E-safety and Internet Use consent form.

4.2 Assessing Risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.
- The Headteacher will ensure that the E-safety Policy is implemented and compliance with the policy monitored.

4.3 Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- 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 policy.
- E-safety complaints are reviewed and the E-safety policy and curriculum planning is adapted accordingly.

Communications Policy

5.1 Introducing the E-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- An E-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- The school will support and encourage E-safety through themed events such as 'Internet Safety Day'.

- Pupils are encouraged to play an active role in the development of the E-safety policy through the School Council.

5.2 Staff and the E-safety policy

- All staff will be given the school E-safety policy and its importance explained alongside associated documents e.g. the child protection policy, behaviour policy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will sign the Warwickshire Acceptable Use Policy, including regular before, during and after school club teachers.
- All staff will ensure their personal telephones or other devices capable of taking photographs or videos will not remain in the classroom during teaching hours but will be stored in secure lockers provided in the staffroom.
- All staff will be given an induction pack that includes;
  - The E-safety policy.
  - The Warwickshire Acceptable Use Policy.
  - Notification of the safeguarding officers.
  - Procedures to follow for reporting.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the school's E-safety Policy on the school website, in newsletters and the school brochure.
- Parents will have opportunities to attend e-safety sessions in school led by either an internally trained safeguarding officer or a member of the Local Authority.
- Parents are regularly asked for their opinion regarding the E-safety provision and are given the opportunity to offer suggestions which could develop it further.

5.4 Visitors and the E-Safety Policy

- All visitors will be provided with an E-Safety leaflet outlining the basic guidelines of this policy.

SEN

The school strives to enable all pupils to reach their full potential. Staff will plan for those needing extra support where needed. The pupils are supported by teachers, ancillary helpers and outside agencies. E-safety is differentiated and supported by teachers or TA's e.g. widgets accompanying e-safety reminders.

Equal Opportunities

The Policy reflects the school policy on equal opportunities and inclusion, where all children, irrespective of religion, age, gender, ethnicity, language or disability have an equal entitlement to receive a quality of education, covering the full extent of the curriculum.

Health and Safety

In-line with ECM 1 and 2, school systems will comply with this policy, Health and Safety Policy and associated risk assessments.

Race Leys Infant School

E-safety Incident Report

Name of school: _____

This Event Report Form Compiled By: **Name** **Title** **Date**	
Staff informed: (Name & Date) **Headteacher** **e-safety co-ordinator** **Child protection officer** **Other**	
Nature of Concern: **Who was involved: pupil/staff/parents?**	
Where did it occur: home, school?	
Time and date of Incident:	
Time and date the incident was logged:	
Action taken: (please tick) **Evidence preserved** **Senior staff informed**	

Other action	
Incident witnessed by: **Staff** **Pupil** **Parent** **Other**	
Other Officers Involved in Response: **LA Officer** **LADO** **NCC Network Security Manager** **Other**	
Follow up Action:	
Evidence Collected (and where retained):	
Review Date if required:	

Race Leys Infant School E-safety Agreement Form For School Staff

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that the network is the property of the school and agree that any use of this network must be compatible with my role.
- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I understand and agree that the school may monitor my network and Internet use to ensure policy compliance.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted its owner.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises.
- I will report any incidents of concern to the school's Designated Child Protection Coordinator (Jen Langtree) or E-safety Coordinator (Karen Sewell) as appropriate.
- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be misinterpreted.
- I will promote E-safety with the students that I work with and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.
- I will ensure that mobile phones are locked away and that they are only used in the staffroom during lunch times.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: ……..…….…… Capitals: ……

Accepted for School: ……. Capitals: ……..

Date: ……..……..

.

Warwickshire County Council