Even Swindon Primary School
Pasture Close, Raybrook Park, Swindon, SN2 2UJ Tel: 01793 523041
email: admin@evenswindon.co.uk www.evenswindon.co.uk

Even Swindon Primary School
Online Saftey Policy
Written: October 2020 Reviewed: October 2022

1.1 Who will write and review the policy?

- The school has appointed an Online Safety Coordinator.
- The Online Safety Policy and its implementation will be reviewed annually.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.
- The School has appointed a member of the Governing Body to take lead responsibility for Online Safety
- This policy is part of a group of computing Policies, such as *Acceptible Use Policy*, *Remote Education Good Working Practice*, *Remote Learning for Parents* and our *Social Media Policy*. This policy refers directly to the online safety and protection of our stakeholders.

1.2 Teaching and learning

1.2.1 Why is Internet use important?

• Internet use is part of the statutory curriculum and is a necessary tool for learning.
• The Internet is a part of everyday 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.
• Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
• The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
• Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Swindon Borough Council and DfE;
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.4 How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Computing coordinator/network manager will review system capacity regularly.
- Use of Foldr (shared network access from home) will be for staff access only and data is encrypted.
- The use of user logins and passwords to access the school network will be enforced.

1.3.2 How will email be managed?

- Pupils have not got access to school based emails.
- Pupils must immediately tell a designated member of staff if they receive offensive email from a personal email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending when appropriate.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use school emails for personal correspondence and personal online accounts.
- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam.
- The head teacher will oversee the editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

• The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.3.4 Can pupils' images or work be published?

• Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
• Pupils work can be published without the permission or the parents. Full names will not be published.
• Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
• The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

1.3.5 How will social networking, social media and personal publishing be managed?

• The school will control access to social media and social networking sites.
- The head teacher and Strategic SLT has control of Twitter and Facebook contents.
- School's YouTube account will be managed by our IT Technician; all videos are unlisted so can't be linked.

• Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
• Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
• Staff official blogs or Instagram should be password protected and run from the school website, or using school email addresses to set them up, with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
• Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible. Please see Remote Education Good Working Practice document and Remote Education Policy.
• Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

1.3.6 How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with Swindon Borough Council and the SWGFL to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Swindon Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 How will videoconferencing be managed?

- Videoconferencing is an important part of distance and remote education.
- All policies linked to Office 365 and Zoom have been set to directly compliment government guidelines linked to videoconferencing.
- Teachers should always record the conference when phoning a pupil or a group.
- All pupil devices will have videoconferencing features blocked or removed.

- Further advice on videoconferencing can be found in our Remote Education Good Working Practice document.

1.3.8 How are emerging technologies managed?

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

1.3.9 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

• The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
• All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
• Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
• All visitor to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.
• Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
• When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
According to Setting Type
• At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
• At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

1.4.2 How will risks be assessed?

• The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never

occur via a school computer. Neither the school nor Swindon Council can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Swindon Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection on our CPOMs system.
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the Local e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Swindon.

1.4.4 How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All Online Safety complaints and incidents will be recorded by the school, on CPOMs, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.5 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

1.4.6 How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.
- Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

1.4.7 How will iPads be managed throughout the school

- iPads are locked down and only Network manager has access to management software (Apple Configurator 2)
- Pupils are unable to download or update apps.
- Data removed from all iPads every 2 terms.
- Staff have free access to downloading on iPads but all apps and contents. should be appropriate for education and age appropriate.
- The Head teacher reserves the rights to remove teacher's iPad at any time to be checked.
- For further uses of iPads see AUP for pupils and staff.

1.4.8 How will mobile phones and personal devices be managed?

- Mobile phones and/or personal devices are not to be brought onto school premises and/or used by children, unless specific permission is granded by the headteacher and the device is locked away during the school day.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

• Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
• The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Pupils Use of Personal Devices:

• If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
• Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

Staff Use of Personal Devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile phones may only be used in the staff room or outside of the school grounds and kept away from children during the school day unless the phone is a school phone or exception reasons, where the Head Teacher will decide.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

1.4.9 Parent and family use of electronic devices

- Mobile phones and other electronic devices are not permitted to be used anywhere in the school or on school grounds by parents and carers. Parents and carers wishing to make phone calls, text or use the internet, must do outside of the school site. This is in line with the safeguarding of our staff and pupils.
- Classroom volunteers must abide by the same mobile device rulings as staff; mobile phones and personal electronic devices but not be used at all during time supporting in the school.
- Parents are not permitted to take photos of the school or the children inside the school without consent from the Head teacher.
- When helping on school trips, parents, carers and other volunteers must not use their mobile phones or other personal device, this includes updating

parents by text or via social media. All communication will be from parent mail or school's twitter account.

- Some events photographs will be permitted. Parents and carers may take photos but they are for personal use and no photo should be uploaded to any social media platform. This include photos of your own pupil anywhere on the school site. At times parents and carers are expected to sign to say they will abide by the policy.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

• All users will be informed that network and Internet use will be monitored.
• An e-Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
• Pupil instruction regarding responsible and safe use will precede Internet access.
• An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
• e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
• e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
• Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 How will the policy be discussed with staff?

• The e-Safety Policy will be formally provided to and discussed with all members of staff.
• To protect all staff and pupils, the school will implement Acceptable Use Policies.
• Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
• Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
• Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
• The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
• All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or

institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This will include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e-Safety will be made available to parents I a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "e-Safety Contacts and References section".

Policy Review

This policy will be reviewed at least every 2 years.

Signed: _____ Chair of Governors

Date: October 2020